Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Am 27. April 2016 wurde die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1 (in der Fassung der Berichtigung ABl. Nr. L 314 vom 22.11.2016 S. 72), beschlossen. Die Datenschutz-Grundverordnung (DSGVO) ist am 25. Mai 2016 in Kraft getreten, kommt ab 25. Mai 2018 zur Anwendung und hebt mit 25. Mai 2018 die Richtlinie 95/46/EG auf.

Der sachliche Anwendungsbereich der DSGVO ist umfassend. Die DSGVO gilt gemäß Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Gemäß Art. 2 Abs. 2 lit. d gilt die DSGVO nicht für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Wenngleich die DSGVO unmittelbare Geltung erlangt, bedarf sie in zahlreichen Bereichen der Durchführung ins innerstaatliche Recht (zB die Errichtung der Aufsichtsbehörde nach Art. 51 Abs. 1 iVm Art. 54 Abs. 1 lit. a DSGVO). Darüber hinaus enthält die DSGVO auch Regelungsspielräume („Öffnungsklauseln“), die fakultativ von den Mitgliedstaaten genutzt werden können. Während die notwendige Durchführung der DSGVO überwiegend im Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, in der Fassung des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, erfolgt, werden Öffnungsklauseln nur zu einem geringen Teil direkt im DSG geregelt.

Der überwiegende Teil der Öffnungsklauseln fällt nicht in den Bereich der allgemeinen Angelegenheiten des Datenschutzes, deshalb werden diese nicht im DSG geregelt. Jedoch kann – soweit erforderlich – in spezifischen Materiengesetzen eine entsprechende Festlegung erfolgen (siehe dazu den Bericht des Verfassungsausschusses zur Regierungsvorlage des Datenschutz-Anpassungsgesetzes 2018 (1761 BlgNR 25. GP 1), welcher zB auf Art. 23 DSGVO hinweist, wonach durch Rechtsvorschriften der Union oder der Mitgliedstaaten die Pflichten und Rechte gemäß den Art. 12 bis 22 und 34 DSGVO unter bestimmten Voraussetzungen gesetzlich beschränkt werden können).

Aus diesen Gründen sind umfassende Änderungen im innerstaatlichen Datenschutzrecht erforderlich, die hinsichtlich der allgemeinen Angelegenheiten des Datenschutzes bereits durch die Erlassung des Datenschutz-Anpassungsgesetzes 2018 vorgenommen wurden, im Hinblick auf die spezifischen Datenverarbeitungen in den jeweiligen Materiengesetzen jedoch noch ausstehen und nun gesammelt im gegenständlichen Sammelgesetz erfolgen sollen. Dabei sollen die materienspezifischen Datenschutzregelungen mit der neuen datenschutzrechtlichen Terminologie in Einklang gebracht werden sowie die sonstigen formellen und inhaltlichen Adaptierungen erfolgen. Im Hinblick auf das unionsrechtliche Transformationsverbot sollen jedoch nur die unbedingt erforderlichen Durchführungsreglungen zur DSGVÜ erlassen werden bzw. sollen Abweichungen nur im Falle materienspezifischer Notwendigkeit erfolgen.

Die Mitgliedstaaten können zudem gemäß Art. 6 Abs. 2 DSGVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten zur Erfüllung von Art. 6 Abs. 1 lit. c und e DSGVO beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX der DSGVO.

Die materienspezifischen Anpassungen an die DSGVO sollen gleichzeitig mit der Anwendung der DSGVO und dem Datenschutz-Anpassungsgesetz 2018 am 25. Mai 2018 in Kraft treten.

Weiters wurde mit dem Datenschutz-Anpassungsgesetz 2018 im DSG die – am gleichen Tag wie die DSGVO beschlossene – Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4.5.2016 S. 89, ins innerstaatliche Recht umgesetzt.

Im 3. Hauptstück des DSG finden sich explizite Regelungen zur Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung (§§ 36 ff). Wie im Bericht des Verfassungsausschusses (1761 BlgNR 25. GP 18) ausdrücklich klargestellt wird, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. Die Anpassungen dieser materienspezifischen Regelungen erfolgen ebenfalls im Rahmen des gegenständlichen Sammelgesetzes (siehe etwa die vorgesehenen Regelungen in der Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631/1975, oder im Gerichtsorganisationsgesetzes (GOG), RGBl. Nr. 217/1896).

Die vorgesehenen Anpassungsbestimmungen sollen durchwegs mit 25. Mai 2018 in Kraft treten. Nur in Einzelfällen ist ein früheres (zB bei redaktionellen Änderungen der der Kundmachung folgende Tag) oder ein späteres (bei Anpassung noch nicht in Kraft stehender Bestimmungen) vorgesehen.

Kompetenzgrundlagen:

Die Kompetenzgrundlagen der vorgeschlagenen Regelungen entsprechen im Wesentlichen jenen der zahlreichen geänderten Bundesgesetze und umfassen daher verschiedenste Tatbestände der Kompetenzartikel der Bundesverfassung. Sie sind ausnahmsweise jeweils im Besonderen Teil angeführt.

Besonderer Teil

Zum 1. Hauptstück (Bundeskanzleramt)

Allgemeines:

Aufgrund der im Allgemeinen Teil genannten neuen datenschutzrechtlichen Vorgaben haben die gesetzlich geregelten Datenverarbeitungen ab dem 25. Mai 2018 den durch die Datenschutz-Grundverordnung geänderten Anforderungen zu genügen, weshalb etliche Materiengesetze, die in den legistischen Zuständigkeitsbereich des Bundeskanzleramtes fallen, anzupassen sind. Da gemäß § 69 Abs. 8 DSG – im Rahmen der europa- und verfassungsrechtlichen Vorgaben – vom DSG abweichende Regelungen in Bundes- und Landesgesetzen zulässig sind, sollen die einschlägigen materienspezifischen Regelungen im Bereich des Datenschutzes als leges speciales den allgemeinen Regelungen des neuen DSG vorgehen.

Im Hinblick auf die Verbote der speziellen Transformation, der inhaltlichen Präzisierung sowie der inhaltlichen Wiederholung einer EU-Verordnung sollen nur die unbedingt erforderlichen Regelungen der Verordnung durchgeführt werden bzw. sollen Abweichungen nur im Falle materienspezifischer Notwendigkeit erfolgen. Das bisher vorgesehene Datenschutzniveau soll dabei jedoch keinesfalls unterschritten werden.

Insbesondere ist beabsichtigt, die derzeitigen Anforderungen für Datenverarbeitungen – z. B. im Hinblick auf Verarbeitungszweck und öffentliches Interesse – zu konkretisieren, um die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 lit. e der Datenschutz-Grundverordnung zu gewährleisten. Darüber hinaus soll der in der Verordnung normierte Grundsatz der Transparenz für die Betroffenen in den Regelungen Berücksichtigung finden. Zudem ist beabsichtigt, die in den Materiengesetzen vorgesehenen Übermittlungsnormen an die neuen Vorgaben anzupassen.

Die in den Materiengesetzen vorgesehenen Datensicherheitsmaßnahmen werden zudem im Hinblick auf die neuen Datensicherheitsbestimmungen in Art. 32, die im Anwendungsbereich der Datenschutz-Grundverordnung unmittelbar zur Anwendung gelangen, angepasst.

Überdies sollen die materienspezifischen Datenschutzregelungen mit der neuen datenschutzrechtlichen Terminologie in Einklang gebracht werden sowie eine Adaptierung der bisherigen Verweise erfolgen.

Zum 1. Abschnitt (Kunst und Medien)

Zu Art. 1 (Änderung des Bundesarchivgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 13 (wissenschaftlicher und fachtechnischer Archiv- und Bibliotheksdienst, Angelegenheiten der

künstlerischen und wissenschaftlichen Sammlungen und Einrichtungen des Bundes), Art. 10 Abs. 1 Z 16 (Einrichtungen der Bundesbehörden und sonstigen Bundesämter), Art. 17 und soweit sich der Gesetzentwurf auf die durch Bundesgesetz eingerichteten juristischen Personen öffentlichen Rechts bezieht, stützt er sich auf die entsprechende Kompetenzbestimmung, auf der das betreffende Gesetz beruht, mit dem die betreffende Einrichtung errichtet wurde,

Zu Art. 1 Z 1 bis 6 (§ 5 Abs. 2 und 3, 7 Abs. 1 und 4, 8 Abs. 5 sowie § 11 Abs. 1):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Gemäß Art. 4 Z 1 der Datenschutz-Grundverordnung sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Die vorgeschlagene Ergänzung des § 5 Abs. 3 1. Satz stützt sich auf Art. 5 Abs. 1 lit. b der Datenschutz-Grundverordnung, wonach personenbezogene Daten grundsätzlich nur für die Zwecke verwendet werden dürfen, für die sie erhoben wurden, Die Verwendung dieser Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke ist jedoch mit den ursprünglichen Zwecken vereinbar.

Weiters sind gemäß Art. 5 Abs. 1 lit. e der Datenschutz-Grundverordnung die personenbezogenen Daten in einer Form zu speichern, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich sind; personenbezogene Daten dürfen jedoch für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke länger gespeichert werden.

Die Ergänzung des § 5 Abs. 3 2. Satz ist zur Klarstellung in Bezug auf den Datenschutzverantwortlichen erforderlich, da Bundesdienststellen dem Österreichischen Staatsarchiv vielfach Schriftgut übergeben, dieses aber nicht zur Übernahme anbieten.

Verantwortliche gemäß Art. 4 Z 7 iVm Art. 26 Abs. 1 der Datenschutz-Grundverordnung sind die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Das Österreichische Staatsarchiv darf erst nach Übernahme des betreffenden Schriftgutes über dessen Verarbeitung entscheiden.

Die vorgeschlagene Änderung des Einleitungssatzes im § 7 Abs. 1 ist erforderlich, da das mit 25. Mai 2018 in Kraft tretende Datenschutzgesetz, BGBl I Nr. 120/2017 generell kein Auskunftsrecht der betroffenen Personen normiert. Dieses Recht ergibt sich unmittelbar aus Art. 15 der Datenschutz-Grundverordnung. Nach Artikel 89 Abs. 2 und 3 der Datenschutz-Grundverordnung können die Auskunfts- und Informationsrechte der betreffenden Personen zu personenbezogenen Daten durch die Mitgliedstaaten eingeschränkt werden, wenn diese für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke verarbeitet werden und die Auskunfts- und Informationspflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Das im derzeit geltenden § 7 Bundesarchivgesetz normierte Recht auf Auskunft und Gegendarstellung kann daher weiter in Geltung stehen.

Zu Art. 1 Z 7 (§ 19 Abs. 3):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 2 (Änderung des Bundesstatistikgesetzes 2000)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 13 (Volkszählungswesen sowie – unter Wahrung der Rechte der Länder, im eigenen Land jegliche Statistik zu betreiben – sonstige Statistik, soweit sie nicht nur den Interessen eines einzelnen Landes dient) und Art. 17 B-VG (Stellung des Bundes als Träger von Privatrechten).

Zu Art. 2 Z 3 (§ 3 Z 3 des Bundesstatistikgesetzes 2000):

Nach Art. 3 Z 6 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken ist eine „Statistische Einheit“ die Grundbeobachtungseinheit, das heißt eine natürliche Person, ein Haushalt, ein Wirtschaftsteilnehmer oder eine sonstige Unternehmung, auf die sich die Daten beziehen.

Zu Art. 2 Z 4 (§ 3 Z 15 des Bundesstatistikgesetzes 2000):

Nach Art. 1 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken schafft diese Verordnung einen Rechtsrahmen für die Entwicklung, Erstellung und Verbreitung europäischer Statistiken.

Gemäß Art. 3 der Datenschutz-Grundverordnung ist diese Verordnung auf die Verarbeitung von personenbezogenen Daten natürlicher Personen anzuwenden.

Gemäß Art. 4 Z 1 der Datenschutz-Grundverordnung sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

In Kapitel XI der Datenschutz-Grundverordnung sind zwar Abgrenzungsregelungen zu anderen Rechtsnormen enthalten, eine solche Regelung besteht in Bezug auf die Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken nicht.

Beide Verordnungen bestehen somit nebeneinander, wobei bei der Verarbeitung von personenbezogenen Daten primär die Datenschutz-Grundverordnung gilt, sofern die Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken nicht spezielle Regelungen für die Verarbeitung von personenbezogenen Daten enthält.

Dafür spricht, dass die Datenschutz-Grundverordnung in Bestimmungen vielfach auf die Verarbeitung von personenbezogenen Daten für statistische Zwecke Bezug nimmt (z. B. Art. 5 Z 1 lit. b und c, Art. 9 Abs. 2 lit. j, Art. 14 Abs. 5 lit. b, Art 17 Abs. 3 lt. d, Art. 89).

Im Erwägungsgrund 163 der Datenschutz-Grundverordnung wird darauf hingewiesen, dass die Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken genauere Bestimmungen zur Vertraulichkeit europäischer Statistiken enthält. Dadurch wird deutlich, dass sich die Vertraulichkeitsregelungen der Verordnung (EG) Nr. 223/2009 nicht auf die Verarbeitung von personenbezogenen Daten an sich, sondern auf das statistische Ergebnis und den darin enthaltenen personenbezogenen Daten bezieht. Im Vorfeld der Verarbeitung von personenbezogenen Daten für die Statistiken gilt daher die Datenschutz-Grundverordnung.

Gemäß Art. 3 Z 7 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken sind „vertrauliche Daten“ Daten, die eine direkte oder indirekte Identifizierung statistischer Einheiten möglich machen und dadurch Einzelinformationen offenlegen. Bei der Entscheidung, ob eine statistische Einheit identifizierbar ist, sind alle Mittel zu berücksichtigen, die nach vernünftigem Ermessen von einem Dritten angewendet werden könnten, um die statistische Einheit zu identifizieren.

Gemäß Art. 3 Z 6 dieser Verordnung ist die „Statistische Einheit“ die Grundbeobachtungseinheit, das heißt eine natürliche Person, ein Haushalt, ein Wirtschaftsteilnehmer oder eine sonstige Unternehmung, auf die sich die Daten beziehen.

Damit ist der Begriff „vertrauliche Daten“ der weitere Begriff als der Begriff „personenbezogene Daten“ nach der Datenschutz-Grundverordnung, da dieser nur Daten natürlicher Personen umfasst.

Nach Art. 20 Abs. 2 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken dürfen vertrauliche Daten, die ausschließlich für die Erstellung europäischer Statistiken erhoben wurden, von den „Nationalen Statistischen Ämtern“ und anderen einzelstaatlichen Stellen und von der Kommission (Eurostat) ausschließlich für statistische Zwecke verwendet werden, es sei denn, die statistische Einheit hat unmissverständlich ihre Zustimmung zur Verwendung der Daten zu anderen Zwecken erteilt.

Gemäß Art. 23 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken darf Wissenschaftlern, die für wissenschaftliche Zwecke statistische Analysen durchführen, Zugang zu vertraulichen Daten, die nur die indirekte Identifikation der statistischen Einheiten ermöglichen, gewährt werden. Diese Regelung für den Zugang von Wissenschaftlern zu den in Rahmen von Statistiken erhobenen personenbezogenen Daten ist damit restriktiver als nach der Datenschutz-Grundverordnung.

Zu Art. 2 Z 5 (§ 4 Abs. 3 Z 8 des Bundesstatistikgesetzes 2000):

Die Differenzierung zwischen Daten natürlicher Personen und Daten von Unternehmen ist erforderlich, da nach der Datenschutz-Grundverordnung der Begriff „personenbezogene Daten“ auf Daten natürlicher Personen eingeschränkt ist. Ist das Unternehmen eine natürliche Person ist zwischen Daten der natürlichen Person und den Unternehmensdaten streng zu differenzieren, wobei nur die Identifikationsdaten (Name uä) des Unternehmens mit den Identifikationsdaten der betreibenden natürlichen Person identisch sind.

Zu Art. 2 Z 6 bis 9 (Überschrift zu § 5, § 5 Abs. 1 und 2 des Bundesstatistikgesetzes 2000):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 2 Z 10 (§ 5 Abs. 6 des Bundesstatistikgesetzes 2000):

Zum Verhältnis der Begriffe „personenbezogene Daten“ und „vertrauliche Daten“ siehe die Ausführungen unter Z 3.

Soweit Datenverarbeitungen aufgrund EU-rechtlicher Verpflichtungen Österreichs notwendig sind, entzieht sich die Datenfolgenabschätzung der Ingerenz Österreichs. Diese hätte das normerlassende EU-Organ (Europäische Kommission oder EU-Rat) bei der Normerlassung vorzunehmen, da die Datenschutz-Grundverordnung für die Organe der EU auch gilt. Außerdem werden in den betreffenden EU-rechtlichen Verpflichtungen um einen einheitlichen europäischen Standard im Bereich der Statistik sicherzustellen, festgelegt, welche personenbezogenen bzw. unternehmensbezogene Daten für die jeweilige Statistik durch die einzelnen nationalen statistischen Ämtern –NSÄ (in Österreich vornehmlich die Bundesanstalt Statistik Österreich) zu erheben sind.

In § 5 Abs. 1 iVm § 4 Abs. 1 und § 8 Abs. 1 ist klargestellt, dass die personenbezogene und unternehmensbezogene Erhebung von Daten nur vorgenommen werden darf, soweit eine solche durch einen innerstaatlich unmittelbar wirksamen internationalen Rechtsakt (EU-Verordnung, EU-Richtlinie, durch Bundesgesetz oder durch eine Verordnung des zuständigen Bundesministers angeordnet ist. Da derartige Rechtsakte im Amtsblatt der Europäischen Gemeinschaften bzw. im Bundesgesetzblatt kundgemacht sind, besteht größtmögliche Transparenz in diesem Bereich über die Befugnisse der Organe der Bundesstatistik (z,B Bundesanstalt Statistik Österreich).

Weiters wird im Bundesgesetz zwischen personenbezogenen Daten natürlicher Personen und unternehmensbezogenen Daten unterschieden.

Diese Unterscheidung dient der größeren Datensicherheit vor allem der personenenbezogenen Daten natürlicher Personen. Natürliche Personen führen vielfach auch Unternehmen. Man denke in diesem Zusammenhang beispielsweise an Ärzte, Steuerberater, Ziviltechniker uä. Würde eine Unterscheidung wischen personenbezogener Daten natürlicher Personen und unternehmensbezogener Daten erfolgen, so käme es zu einer Vermengung von für statistische Zwecke erhobenen höchst persönlichen Daten (zB Familienstand, private Wohnadresse, Kinder, Bildungsdaten uä) und der Unternehmensdaten der betroffenen natürlichen Person.

Aus diesem Grunde ist im vorgeschlagenen § 15 Abs. 1 normiert, dass unverzüglich nach der Erhebung von personenbezogenen Daten natürlicher Personen deren Identitätsdaten zu beseitigen und durch das bereichsspezifische Personenkennzeichen Amtliche Statistik (bPK-AS) zu ersetzen sind. Die Bundesanstalt darf weiters keine Aufzeichnungen führen, aus denen hervorgeht, welcher natürlichen Person welches bPK-AS zuzuordnen ist. Die Identitätsdaten der natürlichen Personen sind nicht mit dem bPK-AS zu ersetzen, sondern zu verschlüsseln, wenn die betreffenden personenbezogenen Daten für die im § 15 Abs. 2 taxativ aufgezählten statistischen Zwecke weiter benötigt werden.

Nach der Erhebung unternehmensbezogener Daten (somit auch jener Unternehmensdaten der natürlichen Personen) ist die Identität des Unternehmens zu löschen oder ebenfalls zu verschlüsseln, wenn dies Daten für weiter Unternehmensstatistiken benötigt werden § 15 Abs. 2).

Die Schlüssel sind getrennt von den verschlüsselten Daten aufzubewahren (§ 15 Abs. 3) und die Entschlüsselung der Daten darf nur für die im Gesetz aufgezählten statistischen Zwecke erfolgen. Die Entschlüsselung wird von der Bundesanstalt protokolliert. Bedienstete der Bundesanstalt haben nur Zugang zu jenen Daten, die sie für die Wahrnehmung ihrer dienstlichen Aufgaben benötigen. Die Zugriffe werden im EDV-Protokoll festgehalten.

Schließlich ist in § 17 eine besondere gerichtliche Strafbestimmung für den Fall der Verletzung des Statistikgeheimnisses normiert.

Zu Art. 2 Z 11 (§ 8 Abs. 2 des Bundesstatistikgesetzes 2000):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 2 Z 12 (§ 15 des Bundesstatistikgesetzes 2000):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung. Außerdem sind die Änderungen erforderlich, da nach der Datenschutz-Grundverordnung der Begriff „personenbezogene Daten“ auf Daten natürlicher Personen eingeschränkt ist und andererseits aufgrund der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken die Vertraulichkeit auch von unternehmensbezogenen Daten sicherzustellen ist.

Die in Abs. 1 vorgesehene Nichtanwendung der Art. 15 (Auskunftsrecht der betroffenen Personen), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 der Datenschutz-Grundverordnung (Recht auf Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten) ist in Art. 89 Abs. 2 der Datenschutz-Grundverordnung gedeckt, da diese Rechte aufgrund der Vielzahl, Vielfalt und des Umfangs der im Zuge der statistischen Erhebungen anfallenden personenbezogenen Daten ernsthaft die Verarbeitung dieser Daten für statistische Zwecke beeinträchtigen würden. Vor allem Verfahren im Zusammenhang mit den Rechten auf Berichtigung, auf Einschränkung der Verarbeitung und Widerspruch gegen die Verarbeitung würde die nach den EU-Vorgaben geforderte rechtzeitige Erstellung von Statistiken gefährden, wenn von diesen Rechten in einer Mehrzahl Gebrauch gemacht wird.

Außerdem kann dem Recht auf Auskunftserteilung nur mit großem Verwaltungsaufwand nachgekommen werden, da die von den Organen der Bundesstatistik erhobenen Daten nach Abs. 1 bis 3 unverzüglich zu verschlüsseln sind und diese zur Auskunftserteilung erst in jedem Einzelfall aufwändig zu entschlüsseln wären, um den Personenbezug wiederherzustellen.

Das Recht auf Berichtigung kann überdies bei den Organen der Bundesstatistik nicht durchgesetzt werden, da die Daten bei den betroffenen Personen unmittelbar erhoben wurden und somit von diesen selbst stammen oder als Verwaltungsdaten bei Behörden oder aus öffentlichen Registern erhoben werden. Das Recht auf Berichtigung müsste der Betroffene daher bei der betreffenden Behörde oder beim betreffenden öffentlichen Register geltend machen.

Ein Widerspruch gegen die Verarbeitung der personenbezogenen Daten geht ebenso ins Leere, da nach Art. 20 Abs. 2 der Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken diese Daten ausschließlich für statistische Zwecke verwendet werden dürfen und die Erstellung von Statistiken gemäß § 4 einer Anordnung durch einen innerstaatlich unmittelbar wirksamen internationalen Rechtsakt, durch Bundesgesetz oder durch Verordnung bedarf.

Zu Art. 2 Z 13 und 14 (§ 17 Abs. 1 bis 3 des Bundesstatistikgesetzes 2000):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 2 Z 15 (§ 24 Z 7 des Bundesstatistikgesetzes 2000):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken.

Zu Art. 2 Z 16 (§ 25a Abs. 1 und 3 des Bundesstatistikgesetzes 2000):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 2 Z 17 (§ 26 Abs. 1 des Bundesstatistikgesetzes 2000):

Die Änderung ist durch die vorgeschlagene Änderung des § 15 Abs. 2 Z 5 bedingt.

Zu Art. 2 Z 18 bis 20 (§ 27 Abs. 2 und 3 sowie § 31 des Bundesstatistikgesetzes 2000):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 2 Z 22 (§ 73 Abs. 10 des Bundesstatistikgesetzes 2000):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 3 (Änderung des Informationssicherheitsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 2 B-VG („äußere Angelegenheiten"), Art. 10 Abs. 1 Z 6 B-VG („Strafrechtswesen"), Art. 10 Abs. 1 Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit einschließlich der ersten allgemeinen Hilfeleistung, jedoch mit Ausnahme der örtlichen Sicherheitspolizei") und Art. 10 Abs. 1 Z 15 B-VG („militärische Angelegenheiten").

Zu Art. 3 Z 1 bis 2 (§ 3 Abs. 3 sowie § 12 Abs. 4b):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Zu Art. 3 Z 3 (§ 18):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 4 (Änderung des Künstler-Sozialversicherungsfondsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 13 B-VG („Stiftungs- und Fondswesen") und Art. 17 B-VG („Stellung des Bundes als Träger von Privatrechten").

Zu Art. 4 Z 1 bis 4 (§ 13):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung.

Die Ergänzung des Abs. 1 durch die Z 8 ist erforderlich, da nach § 25c iVm § 25a Z 1, 3 und 4 Künstlerinnen/Künstler im Krankheitsfall unter bestimmten Voraussetzungen Beihilfen zur Deckung des notwendigen Lebensunterhalts, für Medikamente und medizinische Behandlungen und Kuraufenthalte beim Fond ansprechen können. Um das Vorliegen der gesetzlichen Voraussetzungen für die Gewährung der Beihilfe beurteilen zu können, müssen Gesundheitsdaten der betroffenen Künstlerinnen/Künstler verarbeitet werden Die betreffende Bestimmung soll die gesetzliche Voraussetzung hiefür im Sinne der Datenschutz-Grundverordnung schaffen.

Zu Art. 4 Z 2 (§ 30 Abs. 9):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 5 (Änderung des Mediengesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 6 B-VG („Pressewesen").

Zu Art. 5 Z 1 (§ 43b Abs.9):

Der Hinweis auf das am 25. Mai 2018 nicht mehr existente „DSG 2000" hat zu entfallen.

Zu Art. 5 Z 2 (§ 55 Abs. 10):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 6 (Änderung des ORF-Gesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 9 B-VG („Post- und Fernmeldewesen") und auf Art. I Abs. 2 des Bundesverfassungsgesetzes über die Sicherung der Unabhängigkeit des Rundfunks, BGBl. Nr. 396/1974.

Zu Art. 6 Z 1 bis 2 (§ 4f Abs. 2 Z 23 sowie § 18 Abs. 4 zweiter Satz):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung. Im Übrigen handelt es sich um Anpassung an die Terminologie und die Bestimmungen des DSG. Zu den personenbezogenen Daten über das Verhalten des einzelnen Nutzers, aufgrund deren Speicherung eine (unzulässige) Individualisierung erfolgt, zählt etwa der Browser-

Verlauf, die Häufigkeit der Besuche auf einer bestimmten Seite oder die in Suchmaschinen eingegebenen Begriffe, im Zusammenhalt mit einer bestimmten IP-Adresse.

Zu Art. 6 Z 3 (§ 49 Abs. 18):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 7 (Änderung des Presseförderungsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 17 B-VG („Stellung des Bundes als Träger von Privatrechten“).

Zu Art. 7 Z 1 (§ 2 Abs. 5 dritter Satz):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung. Im Übrigen handelt es sich um Anpassung an die Terminologie und die Bestimmungen des DSG.

Zu Art. 7 Z 2 (§ 17 Abs. 8):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 8 (Änderung des Medienkooperations- und -förderungs-Transparenzgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf § 1 Abs. 4 des Bundesverfassungsgesetzes über die Transparenz von Medienkooperationen sowie von Werbeaufträgen und Förderungen an Medieninhaber eines periodischen Mediums (BVG Medienkooperation und Medienförderung – BVG MedKF-T), BGBl. I Nr. 125/2011.

Zu Art. 8 Z 1 (§ 2 Abs. 3 und in § 3 Abs. 3 und 6):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung. Im Übrigen handelt es sich um Anpassung an die Terminologie und die Bestimmungen des DSG.

Zu Art. 8 Z 2 (§ 7 Abs. 4):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zum 2. Abschnitt (Familien und Jugend)

Zu Art. 9 (Änderung des Familienlastenausgleichsgesetzes 1967)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 17 B-VG („Bevölkerungspolitik, soweit sie die Gewährung von Kinderbeihilfen und die Schaffung eines Lastenausgleiches im Interesse der Familie zum Gegenstand hat“).

Zu Art. 9 Z 1 bis 6 (§ 46a):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Datenschutz-Grundverordnung sowie der Präzisierung der Rechtsgrundlagen für die bereits laufende Verarbeitung.

In diesem Zusammenhang ist festzuhalten, dass für die Vollziehung von Belangen des Familienlastenausgleichs durch die Abgabenbehörden die Bundesabgabenordnung Anwendung findet. Insofern gelten die Regelungen der Bundesabgabenordnung über den Datenschutz (vgl. dazu den vorgesehenen Art. 70) auch in Bezug auf die Auszahlung von Beihilfen wie etwa der Familienbeihilfe.

Zu Art. 9 Z 7 (§ 55 Abs. 37):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 10 (Änderung des Kinderbetreuungsgeldgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 17 B-VG („Bevölkerungspolitik, soweit sie die Gewährung von Kinderbeihilfen und die Schaffung eines Lastenausgleiches im Interesse der Familie zum Gegenstand hat“).

Zu Art. 10 Z 1 bis 6 (§ 25 Abs. 2, Überschrift zu § 36, § 36 bis 37b und § 50 Abs. 21):

Mit Einführung des Kinderbetreuungsgeldes im Jahr 2002 wurde bei der Niederösterreichischen Gebietskrankenkasse das Kompetenzzentrum Kinderbetreuungsgeld eingerichtet. Diese hat das EDV-Programm als Informationsverbundsystem entwickelt, auf welches alle administrierenden Krankenversicherungsträger (KV-Träger) zugreifen. Das Kompetenzzentrum fungiert somit als Drehscheibe und wickelt ua auch die Kommunikation mit dem Bundeskanzleramt (FLAF) ab, erstellt Statistiken bzw. ist für die Auszahlung der Leistungen zuständig. Die Verfahren obliegen jedoch den einzelnen Krankenversicherungsträgern, wobei die Niederösterreichische Gebietskrankenkasse somit eine Doppelfunktion als Kompetenzzentrum und als administrierender KV-Träger innehat. In der Folge wurde das Kompetenzzentrum auch noch als Verbindungsstelle im Sinne der Verordnung (EG) Nr. 883/2004 eingerichtet.

Es wird nun eine Anpassung an die DSGVO vorgenommen und eine Kinderbetreuungsgeld-Datenbank eingerichtet, wobei es sich dabei jedoch nur um eine rechtliche Umwandlung des bisherigen Informationsverbundsystems in eine Kinderbetreuungsgeld-Datenbank handelt.

Die Niederösterreichische Gebietskrankenkasse als Kinderbetreuungsgeld-Kompetenzzentrum wird aufgrund ihrer schon bisherigen Sonderrolle als Verantwortliche im Sinne der DSGVO eingesetzt. Sie ist auch für die technische Errichtung, Betreibung, Wartung usw. der Datenbank zuständig, wobei die Daten aus dem bisherigen Informationsverbundsystem in der zukünftigen Datenbank weitergeführt werden, sodass Kontinuität gewährleistet ist.

Die Datenbank wird derart ausgestaltet, dass sowohl die administrierenden Krankenversicherungsträger als auch das Kompetenzzentrum selbst sowie der Hauptverband der Sozialversicherungsträger und die Abgabenbehörden jene personenbezogenen Daten übermitteln, die für den Vollzug des KBGG erforderlich sind. Solche Daten sind also all jene Daten, die benötigt werden, um das Gesetz zu vollziehen, wobei auch auf alle anderen anzuwendenden Bestimmungen wie etwa die europarechtlichen Koordinierungsregelungen (zB Verordnung (EG) Nr. 883/2004), Wiener Konventionen, Amtssitzabkommen usw. Bedacht zu nehmen ist.

Die weitere Verarbeitung erfolgt dann in dieser Datenbank, wobei die Verarbeitung laut DSGVO beispielsweise das Erfassen, die Organisation, das Speichern, die Änderung, das Auslesen, das Abfragen oder etwa den Abgleich der Daten umfasst.

Die von der Niederösterreichischen Gebietskrankenkasse in ihrer Funktion als Kompetenzzentrum oder Verbindungsstelle erhobenen Daten müssen ebenfalls in die Datenbank eingespeist und zur Verfügung gestellt werden. Weiters werden Zugriffs- und Verarbeitungsrechte für alle administrierenden Krankenversicherungsträger und die Niederösterreichische Gebietskrankenkasse in ihren Funktionen als Kompetenzzentrum und Verbindungsstelle geregelt.

Dem Kompetenzzentrum, welches schon bisher mit den Datenmeldungen an das DVR- Register bei der Datenschutzkommission betraut war, obliegt künftig das Führen des Verzeichnisses im Sinne des Art. 30 der DSGVO.

Dem Bundeskanzler sind vom Kompetenzzentrum wie bisher Statistiken aus der Datenbank zur Verfügung zu stellen.

Es handelt sich bei dieser Novelle im Grunde nur um eine terminologische Anpassung an die Begrifflichkeiten der DSGVO.

Die Umwandlung vom Informationsverbundsystem zu einer Datenbank sowie die laufenden Wartungs- und Entwicklungskosten der Datenbank führen nach derzeitigem Kenntnisstand de facto zu keinen Mehrkosten, da es sich um eine rein rechtliche und keine faktische Implementierung einer neuen Datenbank handelt. Die laufende Finanzierung erfolgt wie bisher aus dem Familienlastenausgleichsfonds. Auch etwaige Weiterentwicklungs- und Wartungskosten werden wie bisher aus dem FLAF getragen.

Zu Art. 10 Z 7 (§ 50 Abs. 21):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 11 (Änderung des Bundes-Kinder- und Jugendhilfegesetzes 2013)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 12 Abs. 1 Z 1 B-VG („Mutterschafts-, Säuglings- und Jugendfürsorge sowie Armenwesen“) und Art. 10 Abs. 1 Z 6 B-VG „Zivilrechtswesen“.

Zu Art. 11 Z 1 bis 6 und 8 bis 12, 14, 15 und 17 (§ 8 und 40):

Es wird eine Anpassung an die Terminologie der DSGVO vorgenommen:

Anstelle des Begriffs „Daten“ wird der Begriff „personenbezogene Daten“ verwendet. Eine inhaltliche Änderung erfolgt nicht.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Die begrifflichen Anpassungen sind daher entsprechend vorzunehmen.

Weiters wird auch die Verarbeitung von Video- und Bildmaterial geregelt. Diese Materialien werden zumeist im Rahmen diagnostischer und therapeutischer Settings erstellt und dürfen nur für die in § 40 Abs. 1 und 3 normierten Zwecke (insbesondere Gefährdungsabklärung, Erziehungshilfen, Stellungnahmen an Gerichte) verarbeitet werden. Die Bestimmungen der §§ 12 und 13 DSG sind dabei einzuhalten.

Zu Art. 11 Z 7 und 13 (§ 9 Abs. 4 und § 40 Abs. 5):

Die vorgesehenen Datensicherheitsmaßnahmen werden im Hinblick auf die neuen Datensicherheitsbestimmungen in Art. 32, die im Anwendungsbereich der DSGVO unmittelbar zur Anwendung gelangen, aufgehoben.

Zu Art. 11 Z 19 (§ 40 Abs. 7):

Im Hinblick auf die geplante Weiterentwicklung des automatisierten Familienbeihilfenverfahrens soll auch der Kinder- und Jugendhilfeträger ermächtigt werden, Daten an die Finanzverwaltung weiterzugeben.

Zu Art. 11 Z 21 (§ 47):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 12 (Änderung des Bundesgesetzes über die Einrichtung einer Dokumentations- und Informationsstelle für Sektenfragen)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 17 B-VG („Stellung des Bundes als Träger von Privatrechten“).

Zu Art. 12 Z 1 (§ 5):

Die aus dem Jahr 1998 stammenden Formulierungen sind an die derzeitigen Anforderungen für Datenverarbeitungen – z. B. im Hinblick auf Verarbeitungszweck und Weitergabe von personenbezogenen Daten – zu konkretisieren, um die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 lit. e DSGVO zu gewährleisten.

§ 5 regelt ausdrücklich die Erlangung und Offenlegung von personenbezogenen Daten und trifft geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen, weshalb gemäß Art. 14 Abs. 5 DSGVO die Abs. 1 bis 4 leg. cit. nicht zur Anwendung kommen.

Außerdem wurden insbesondere jene Personen und Institutionen taxativ aufgezählt, an die personenbezogene Daten weitergegeben werden dürfen.

Behörden sind öffentliche Dienststellen, die im Rahmen der Hoheitsverwaltung tätig sind.

Einrichtungen zur Betreuung, Erziehung und zum Unterricht von Minderjährigen sind Organisationen, die nicht nur bestimmte Fertigkeiten vermitteln, wie Tanz- Ski- oder Musikschulen, sondern solche, die sich regelmäßig der ganzheitlichen Erziehung und Betreuung von Kindern und Jugendlichen widmen. Dazu zählen insbesondere Kinderbildungs- und –betreuungseinrichtungen, Schulen, Schülerheime, sozialpädagogische Einrichtungen und Angebote der außerschulischen Jugendarbeit.

Natürliche und juristische Personen, die ein berechtigtes Interesse glaubhaft machen, sind solche, die aufgrund ihrer Lebenssituation Informationen über Sekten oder sektenähnliche Aktivitäten benötigen um

weitere (rechtlich) relevante Entscheidungen oder Maßnahmen zu treffen. Beispiele für solche Personen sind etwa Eltern, deren minderjährige/r Tochter oder Sohn einer Gruppierung beitreten möchte, oder der Betrieb, in dem ein/e Mitarbeiter/in eine Sekte oder sektenähnliche Gemeinschaft bewirbt.

Weiters wird im Sinne des Grundsatzes der Transparenz für die betroffenen Personen erstmals geregelt, welche personenbezogenen Daten von Personen, die Informationen bei der Bundesstelle einholen oder Beratung in Anspruch nehmen, verarbeitet werden dürfen. Diese Personen teilen ihre Daten der Bundesstelle freiwillig mit und können auf Wunsch auch anonym bleiben. Die Dokumentation ist notwendig, um bei mehrfachen Beratungsterminen an Ergebnisse vorangegangener Gespräche anknüpfen zu können oder nachzuvollziehen, welches Informationsmaterial zugesendet wurde. Eine Weitergabe dieser Daten ist im Sinne des Vertrauensschutzes nicht vorgesehen.

Außerdem wird eine Anpassung an die Terminologie der DSGVO vorgenommen:

Das Wort „Betroffener“ wird durch die Wortfolge „betroffene Person“ ersetzt, ohne eine inhaltliche Änderung der Regelung zu bewirken.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Die begrifflichen Anpassungen sind daher entsprechend vorzunehmen.

§ 10 Abs. 1 letzter Satz wird aus systematischen Gründen in den § 5 übernommen.

Zu Art. 12 Z 2 (§ 10 Abs. 1):

Die bereits bisher geübte Praxis im Bericht gemäß § 10 nur anonymisierte Daten zu verwenden, wird nunmehr aus Gründen der Transparenz für betroffene Personen explizit im Gesetz normiert.

Im Hinblick auf den Grundsatz der Eigenverantwortung im Sinne des Art. 5 DSGVO entfällt der Bericht der Bundesstelle für Sektenfragen gegenüber dem zuständigen Bundesminister (jetzt: Bundeskanzler bzw. Bundesministerin für Frauen, Familien und Jugend) sowie die Berichtspflicht des Bundesministers gegenüber dem Datenschutzrat.

Der letzte Satz wird aus systematischen Gründen in den § 5 übernommen.

Zu Art. 12 Z 3 (§ 11):

Untrennbar verbunden mit dem Schutz personenbezogener Daten ist die Festlegung von Verschwiegenheitspflichten. Deshalb wurden diese unter Berücksichtigung der Grundsätze des Art. 5 DSGVO überarbeitet.

Zu Art. 12 Z 4 (§ 13 Abs. 2):

In dieser Bestimmung werden Verweise und die Bezeichnungen der Regierungsmitglieder angepasst.

Zu Art. 12 Z 5 (§ 14):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 13 (Änderung des Bundes-Jugendförderungsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 17 B-VG („Stellung des Bundes als Träger von Privatrechten“).

Zu Art. 13 Z 1 bis 3 (§ 8 Abs. 2 und § 9):

Die Anforderungen für Datenverarbeitungen – zB im Hinblick auf Verarbeitungszweck – sind zu konkretisieren, um die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 lit. e DSGVO zu gewährleisten. Darüber hinaus soll der in der Verordnung normierte Grundsatz der Transparenz für die betroffenen Personen in den Regelungen Berücksichtigung finden.

Daher wird die Ermächtigung zur Regelung des Datenschutzes in den Richtlinien (§ 8) aufgehoben und eine entsprechende Bestimmung direkt in das Gesetz aufgenommen.

Zur Mitgliedschaft zu einer Jugendorganisation gemäß § 2 Abs. 2 können auch Mitgliedschaften zu Teilorganisationen oder regionalen Untergliederungen einer Organisation u.ä. erfasst werden.

Daten zur fachlichen Eignungsprüfung umfassen insbesondere Konzepte, Referenzen und Befähigungsnachweise.

Zu den Daten zur wirtschaftlichen Eignungsprüfung zählen z B Rechnungsabschlüsse, Bilanzen oder Bonitätsauskünfte.

Angaben über Förderungen anderer Gebietskörperschaften und Rechtsträger dienen der Vermeidung von Doppelförderungen für gleichartige Aufgabenbereiche.

Die Gewährung und der Nachweis der widmungsgemäßen Verwendung von Förderungen wird im ELAK des Bundes dokumentiert und entsprechend den Bestimmungen der Büroordnung gelöscht.

Zu Art. 13 Z 4 (§ 12):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 14 (Änderung des Familienzeitbonusgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 11 („Sozialwesen“).

Zu Art. 14 Z 1 bis 3 (§ 4 Abs. 3, § 8, § 9 samt Überschrift):

Es wird eine Anpassung des Familienzeitbonusgesetzes an die DSGVO vorgenommen.

Für den Familienzeitbonus wird keine eigene Datenbank errichtet, sondern werden die Daten in der Kinderbetreuungsgeld-Datenbank verarbeitet. Die diesbezüglichen Bestimmungen im KBGG gelten daher sinngemäß für das FamZeitbG.

Zu Art. 14 Z 4 (§ 12 Abs. 2):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zum 2. Hauptstück (Öffentlicher Dienst)

Allgemeines:

Es werden Anpassungen in den datenschutzrechtlichen Bestimmungen in den Dienstrechten an die Datenschutz-Grundverordnung (DSGVO) vorgenommen.

Im Übrigen wird auf die Ausführungen im Vorblatt verwiesen.

Zu Art. 15 (Änderung des Beamten-Dienstrechtsgesetzes 1979)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 15 Z 1 bis 5, 8, 13 und 17 (§ 48 Abs. 1, Überschrift zu § 79e, § 79e Abs. 2 und 5, § 79g Abs. 1 und § 79h BDG 1979):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 15 Z 6 (§ 79e Abs. 2a BDG 1979):

Die Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit und auch die Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung muss dem jeweils Verantwortlichen jedenfalls möglich sein, um den ihm auferlegten Pflichten nachkommen und die ihm gewährten Rechte ausüben zu können. Dass hierbei auch besondere Kategorien personenbezogener Daten im Falle der unbedingten Erforderlichkeit verarbeitet werden können, wird insbesondere auch im Hinblick auf die ermöglichte private IKT-Nutzung einer Beamtin oder eines Beamten vorgesehen. Die Verarbeitung besonderer Kategorien personenbezogener Daten zu Kontrollzwecken wird auf Art. 9 Abs. 2 lit. b und g DSGVO gestützt. Unbedingt erforderlich ist eine Verarbeitung zu Kontrollzwecken dann, wenn mit der Verarbeitung personenbezogener Daten alleine nicht das Auslangen gefunden werden kann, um Schäden an der IKT-Infrastruktur abzuwehren, ihre korrekte Funktionsfähigkeit zu gewährleisten oder um einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung nachzugehen. Für diesen Fall wird ein entsprechend höheres Schutzniveau für besondere Kategorien personenbezogener Daten vorgesehen. Die Information, dass besondere Kategorien personenbezogener Daten verarbeitet werden, hat sich lediglich allgemein darauf zu beziehen, dass neben personenbezogenen Daten auch besondere Kategorien personenbezogener Daten verarbeitet werden. Direkt zur Verfügung zu stellen bedeutet, dass die die Beamtin oder den Beamten betreffenden Daten des Protokolls ohne Befassung von Zwischenvorgesetzten an sie oder ihn ergehen sollen. Der Beamtin oder dem Beamten sind lediglich die sie oder ihn betreffenden Daten des Protokolls zur Verfügung zu stellen.

Es ist darauf zu achten, dass die Rechte Dritter nicht nachteilig beeinflusst werden, was insbesondere bei namentlicher Nennung Dritter der Fall sein kann.

Zu Art. 15 Z 7 (§ 79e Abs. 3 BDG 1979):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht und die Klarstellung, dass nicht nur Inhalte übertragener, sondern auch zu übertragender Nachrichten unter den angeführten Voraussetzungen kontrolliert werden dürfen.

Zu Art. 15 Z 9 und 11 (§ 79f Abs. 1 und 4 BDG 1979):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht und die Klarstellung, dass kein Bezug auf Inhalte übertragener oder zu übertragender Nachrichten oder auf besondere Kategorien personenbezogener Daten genommen werden darf. Ein allgemeiner Hinweis an die Leiterin oder den Leiter der Dienststelle, dass Inhalte einer übertragenen oder zu übertragenden Nachricht oder besondere Kategorien personenbezogene Daten betroffen sind, ist zulässig.

Zu Art. 15 Z 10 und 14 (§ 79f Abs. 3 und § 79g Abs. 4 BDG 1979):

Die begründeten Ausnahmefälle, in denen ein längerer Beobachtungszeitraum festgesetzt wird, sind schriftlich zu dokumentieren.

Zu Art. 15 Z 12 und 15 (§ 79f Abs. 5 und § 79g Abs. 6 BDG 1979):

Neben terminologischen Anpassungen an das neue Datenschutzrecht wird ein Recht zur Stellungnahme gegenüber der Leiterin oder dem Leiter der Dienststelle eingeführt.

Zu Art. 15 Z 16 (§ 79g Abs. 7 BDG 1979):

Neben terminologischen Anpassungen an das neue Datenschutzrecht wird die Dokumentationspflicht erweitert und ein Recht zur Stellungnahme gegenüber der Leiterin oder dem Leiter der Dienststelle eingeführt.

Zu Art. 15 Z 18 (§ 204 Abs. 7 BDG 1979):

Es werden terminologische Anpassungen an das neue Datenschutzrecht vorgenommen. Neben der Prüfung etwaiger Zulassungserfordernisse sind vor allem die Einholung und Verarbeitung von Strafregistereinkünften gemäß den §§ 9 und 9a des Strafregistergesetzes 1968, BGBl. Nr. 277/1968, sowie die Abfrage und Verarbeitung von Vorwarnungen nach Art. 56a der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen, ABl. Nr. L 255 vom 30.09.2005 S. 22, zuletzt geändert durch den Delegierten Beschluss (EU) 2017/2113, ABl. Nr. L 317 vom 01.12.2017 S. 119, im Binnenmarkt-Informationssystem (IMI) vorgesehen. Diese dienen primär dienstrechtlichen Zwecken und werden von Stellen durchgeführt, deren Hauptaufgaben nicht im Bereich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten liegen, weswegen der Anwendungsbereich der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 04.05.2016 S. 89, ebenso wie bei der bloßen Verarbeitung von Daten zu Strafverfolgungszwecken wie im Falle des § 280 Abs. 3 nicht eröffnet ist. Da Strafregisterauskünfte nach ihrer Überprüfung unverzüglich zu löschen sind, wird im Sinne des Art. 10 DSGVO festgelegt, dass deren Verarbeitung schriftlich zu dokumentieren ist. Dies erfolgt einerseits aufgrund der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und andererseits, um zusammen mit der unverzüglichen Löschung der Strafregisterauskünfte die Rechte und Freiheiten der betroffenen Personen zu garantieren.

Zu Art. 15 Z 19 bis 21 (§ 280, § 280a und § 280b BDG 1979):

Am 27. April 2016 wurde die DSGVO beschlossen. Die DSGVO ist am 25. Mai 2016 in Kraft getreten, tritt am 25. Mai 2018 in Geltung und hebt mit 25. Mai 2018 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23.11.1995 S. 31, in der Fassung der Verordnung (EG) Nr. 1882/2003, ABl. Nr. L 284 vom 31.10.2003 S. 1, auf. Aus diesen Gründen sind Anpassungen in den datenschutzrechtlichen Bestimmungen der jeweiligen Materiengesetze erforderlich.

Die §§ 280 ff und die weiteren datenschutzrechtlichen Bestimmungen sind als leges speciales zu den allgemeinen Regelungen des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, in Zusammenschau mit diesem sowie der DSGVO zu lesen. Auf die Regelung des § 30 Abs. 5 DSG, wonach gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden können, darf an dieser Stelle ebenso wie auf die Begriffsbestimmungen des § 278 hingewiesen werden. Bezüglich der Datenverarbeitung im Beschäftigungskontext wird von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht.

Der Anwendungsbereich der §§ 280 ff erstreckt sich abweichend von § 1 auf alle in § 280 Abs. 1 genannten betroffenen Personen. Die §§ 280 ff beziehen sich ausschließlich auf die erforderlichenfalls durch die Leiterinnen und Leiter der Zentralstellen als jeweils Verantwortliche verarbeiteten, übermittelten und weiterverarbeiteten personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der in § 280 Abs. 1 genannten betroffenen Personen. Diese Bestimmungen regeln folglich ausschließlich das Schicksal dieser durch die Leiterin oder den Leiter der jeweiligen Zentralstelle erforderlichenfalls verarbeiteten, übermittelten und weiterverarbeiteten dienstrechtlichen, arbeits- und sozialrechtlichen, haushaltsrechtlichen, besoldungsrechtlichen, pensionsrechtlichen, organisationsbezogenen, ausbildungsbezogenen und sonstigen mit den angeführten Rechtsverhältnissen in unmittelbarem Zusammenhang stehenden personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der betroffenen Personen. Dem Verantwortlichen gemäß Art. 4 Z 7 DSGVO obliegt die Verantwortung für Verarbeitungen, Übermittlungen und Weiterverarbeitungen durch die ihm zuzuordnenden Stellen oder Personen, beispielsweise ihm unterstellte Bedienstete, eingerichtete Kommissionen, Leiterinnen oder Leiter von Dienststellen oder IT-Stellen. Personenbezogene Daten oder besondere Kategorien personenbezogener Daten von Personen gemäß § 280 Abs. 1 stehen mit einem Rechtsverhältnis in unmittelbarem Zusammenhang, wenn diese Daten bei Außerachtlassung des Rechtsverhältnisses objektiv betrachtet nicht oder nicht in einer solchen Weise verarbeitet, übermittelt oder weiterverarbeitet werden würden, wie sie es bei Berücksichtigung des Rechtsverhältnisses werden würden. Hiefür können etwa mit dem jeweiligen Rechtsverhältnis in unmittelbarem Zusammenhang stehende personenbezogene steuerrechtliche oder personalvertretungsrechtliche Daten angeführt werden. § 280 Abs. 1 und 2 ermächtigt die Leiterinnen und Leiter der Zentralstellen als jeweils Verantwortliche lediglich, die im Beschäftigungskontext erforderlichen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten zu verarbeiten, zu übermitteln und weiterzuverarbeiten.

Zu § 280 Abs. 1 und 2 wird festgehalten, dass eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung und Weiterverarbeitung, sofern nicht ausdrücklich normiert, auf Grundlage des § 280 Abs. 1 und 2 nicht vorgesehen ist. Von der Ermächtigung des § 280 Abs. 1 und 2 zur Übermittlung sind lediglich erforderliche Übermittlungen zwischen den Leiterinnen und Leitern der Zentralstellen erfasst. Jedenfalls erforderlich ist eine Übermittlung, wenn ein Rechtsverhältnis in den Wirkungsbereich einer anderen Leiterin oder eines anderen Leiters einer Zentralstelle übergeht. Die Dokumentation einer Übermittlung an Dritte, die über eine Übermittlung nach § 280 Abs. 1 erster Satz hinausgeht, hat zumindest Datum, Uhrzeit, Empfängerin oder Empfänger, die Kategorien und den Umfang der übermittelten personenbezogenen Daten und besonderen Kategorien personenbezogener Daten und eine Begründung der Übermittlung unter Hinweis auf die jeweilige Rechtsgrundlage zu enthalten. Eine Weiterverarbeitung zu einem anderen Zweck, der ebenso wie der ursprüngliche Zweck der Verarbeitung von § 280 Abs. 2 umfasst sein muss, ist nur möglich, sofern die personenbezogenen Daten oder die besonderen Kategorien personenbezogener Daten zu diesem „neuen“ Zweck ebenfalls erhoben und verarbeitet werden dürften. Eine derartige neuerliche Erhebung bereits vorhandener Daten soll jedoch aus Gründen der Verwaltungsvereinfachung sowie den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit folgend unterbleiben, sofern eine Weiterverarbeitung erfolgen kann und darf. Diesen Grundsätzen sowie der Verwaltungsvereinfachung zu genügen, ist ein wichtiges Ziel des allgemeinen öffentlichen Interesses im Sinne eines wirtschaftlichen und finanziellen Interesses Österreichs, wobei vor allem der Haushalts- und Steuerbereich betroffen sind. Die anderen Zwecke einer Weiterverarbeitung, die nur erforderlichenfalls erfolgen darf, sind bereits in § 280 Abs. 2 dargelegt. Alle diese Zwecke dienen dem übergeordneten Zweck der Personaldatenverarbeitung im jeweiligen Rechtsverhältnis und stehen somit in einem engen und manchmal untrennbaren Zusammenhang. Die Datenerhebung erfolgt zwar jeweils zu einem konkreten Zweck, jedoch stets im Hinblick auf die Personaldatenverarbeitung im jeweiligen Rechtsverhältnis. Personenbezogene Daten und besondere Kategorien personenbezogener Daten werden im Rahmen einer Weiterverarbeitung nur insofern verarbeitet, als eine neuerliche Erhebung der bereits vorhandenen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten möglich wäre. Da Strafregisterauskünfte nach ihrer Überprüfung unverzüglich zu löschen sind, kann eine Weiterverarbeitung selbiger zu einem anderen Zweck gar nicht in Betracht kommen. Aufgrund der genannten Einschränkungen der Weiterverarbeitung resultieren aus einer Weiterverarbeitung für die betroffene Person keine Folgen, die nicht auch ohne die jeweilige Weiterverarbeitung eingetreten wären. Es gelten aus den genannten Gründen außerdem die gleichen Garantien, die im Falle einer Neuerhebung der personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten gelten würden.

§ 280 Abs. 3 ermächtigt jeweils die Leiterinnen und Leiter der Zentralstellen, personenbezogene Daten und besondere Kategorien personenbezogener Daten gemäß § 280 Abs. 1 ausschließlich auf Ersuchen einer zuständigen Behörde gemäß § 36 Abs. 2 Z 7 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, deren Aufgabe die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, die

Strafvollstreckung oder der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit ist, unter den im Gesetz angeführten Voraussetzungen zu verarbeiten. Beispielhaft können als zuständige Behörden kriminalpolizeiliche Behörden oder Justizbehörden, insbesondere Staatsanwaltschaften oder Gerichte, genannt werden. Die Beschränkung der Rechte der betroffenen Person gemäß Art. 23 DSGVO erfolgt im notwendigen und verhältnismäßigen Ausmaß im Rahmen einer Einzelfallprüfung, liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gewährleistet ist. Die zuständige Behörde soll durch die Vornahme der erforderlichen bloßen Verarbeitung durch die Leiterin oder den Leiter der jeweiligen Zentralstelle unterstützt werden. Im Einzelfall ist zu prüfen, in welchem Ausmaß die Rechte der betroffenen Person gemäß Art. 12 bis 14 und Art. 16 bis 22 DSGVO in der Zeit vom Einlangen des Ersuchens bis zum Zeitpunkt der Information der betroffenen Person beschränkt werden müssen, damit die Verwirklichung der Zwecke des Ersuchens nicht unmöglich gemacht oder ernsthaft beeinträchtigt wird. Dabei kommen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zur Anwendung. Da die entsprechenden Beschränkungen der Rechte der betroffenen Person bereits in § 280 Abs. 3 kundgemacht werden und eine Unterrichtung über die Beschränkung im Einzelfall dem Zwecke der Beschränkung abträglich wäre, ist ein Informieren der betroffenen Person erst vorgesehen, sobald es nicht mehr dem Zweck des Ersuchens zuwiderläuft oder zuwiderlaufen kann. Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung ergeben sich aus den jeweiligen Verfahrensrechten. Für den Bereich des § 280 Abs. 3, also der bloßen Verarbeitung aufgrund eines entsprechenden Ersuchens, ist die Leiterin oder der Leiter der jeweiligen Zentralstelle Verantwortlicher. Die Speicherfristen richten sich nach § 280a Abs. 2 bis 5 oder nach den gemäß § 280 Abs. 7 erlassenen Verordnungen. Das Informieren der betroffenen Person gemäß Art. 12 bis 14 DSGVO hat erst nach Mitteilung durch die ersuchende zuständige Behörde an die Leiterin oder den Leiter der jeweiligen Zentralstelle direkt zu erfolgen, was bedeutet, dass es zu keiner Befassung von Zwischenvorgesetzten kommen soll. Zudem wird der betroffenen Person ein Recht zur Stellungnahme gegenüber der Leiterin oder dem Leiter der Dienststelle eingeräumt. § 280 Abs. 3 regelt ausschließlich die bloße Verarbeitung aufgrund eines Ersuchens zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, der Strafvollstreckung oder des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Sonstige Ersuchen sind gemäß § 280 Abs. 1 und 2 oder gemäß ihrer jeweiligen Rechtsgrundlage zu beurteilen.

Da Art. 37 bis 39 DSGVO insbesondere die Stellung sowie die Aufgaben einer oder eines Datenschutzbeauftragten regeln, ist in § 280 Abs. 4 nur noch die formale Zuständigkeit zur Benennung festzulegen. Auf § 5 DSG, der durch § 280 Abs. 4 konkretisiert wird, wird hingewiesen. Wird von den Leiterinnen und Leitern der Zentralstellen jeweils für den Wirkungsbereich des jeweiligen Ressorts nicht eine (gemeinsame) Datenschutzbeauftragte oder ein (gemeinsamer) Datenschutzbeauftragter, sondern werden mehrere Datenschutzbeauftragte benannt, so soll klargestellt sein, dass dies nur nötigenfalls und stets unter dem Aspekt der Aufteilung der Zuständigkeit für den Wirkungsbereich des jeweiligen Ressorts erfolgen soll, sodass auch in diesem Fall immer die Zuständigkeit einer oder eines benannten Datenschutzbeauftragten gegeben ist.

§ 280 Abs. 5 regelt zusätzlich zur bereits bestehenden Einsichtsermächtigung der Bundesministerin oder des Bundesministers für öffentlichen Dienst und Sport im Rahmen der ihr oder ihm in Vorschriften gemäß § 280 Abs. 2 Z 2 übertragenen Mitwirkungsbefugnisse die erforderliche nicht inhaltsändernde Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten zum Zwecke der Sicherung der Datenqualität. Nicht inhaltsändernd bedeutet, dass durch die Verarbeitungen, Übermittlungen und Weiterverarbeitungen die Inhalte der in den Datenverarbeitungssystemen gemäß § 280 Abs. 1 erfassten personenbezogenen Daten und besonderen Kategorien personenbezogener Daten nicht verändert werden. So sollen etwaige im Zuge der Einsichtnahme auftauchende unklare oder missverständliche Daten von der Bundesministerin oder dem Bundesminister für öffentlichen Dienst und Sport als Verantwortlichem erforderlichenfalls überprüft und dem oder den zuständigen Verantwortlichen gemäß § 280 Abs. 1 mitgeteilt werden können. Dieser kann beziehungsweise diese können aufgrund der Mitteilung im Rahmen seiner oder ihrer jeweiligen Verantwortlichkeit tätig werden und die personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten einer Klarstellung zuführen.

Gemäß § 280 Abs. 6 ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport ermächtigt, personenbezogene Daten und besondere Kategorien personenbezogener Daten zusätzlich zur bereits bestehenden Regelung zu statistischen Auswertungen auch zu wissenschaftlichen oder historischen Forschungszwecken unter den angeführten Voraussetzungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten. Soweit hierbei besondere Kategorien personenbezogener Daten verarbeitet, übermittelt oder weiterverarbeitet werden, muss ein schriftlich zu dokumentierendes wichtiges

öffentliches Interesse an der Untersuchung vorliegen. In § 280 Abs. 6 dritter Satz wird von den Öffnungsklauseln in Art. 23 und in Art. 89 Abs. 2 DSGVO Gebrauch gemacht. Es werden die Rechte der betroffenen Personen auf Information, Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch im Rahmen einer Abwägung im jeweiligen Einzelfall beschränkt. Dadurch soll insbesondere sichergestellt werden, dass die für diese Zwecke notwendige Vollständigkeit der Daten gewährleistet und nicht durch Ausübung der genannten Rechte der betroffenen Personen ernsthaft beeinträchtigt oder unmöglich gemacht wird. Regelungen zur Auflösung des Personenbezuges durch geeignete technische Mittel tragen insbesondere dem Grundsatz der Datenminimierung und dem Schutz der Rechte und Freiheiten betroffener Personen Rechnung. Erforderlichenfalls ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport abermals ermächtigt, nicht inhaltsändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen der genannten Daten auch zum Zwecke der Sicherung der Datenqualität vorzunehmen. Nicht inhaltsändernd bedeutet, dass durch die Verarbeitungen, Übermittlungen und Weiterverarbeitungen die Inhalte der in den Datenverarbeitungssystemen gemäß § 280 Abs. 1 erfassten personenbezogenen Daten und besonderen Kategorien personenbezogener Daten nicht verändert werden. So sollen etwaige im Zuge einer beispielsweise statistischen Auswertung auftauchende unklare oder missverständliche Daten von der Bundesministerin oder dem Bundesminister für öffentlichen Dienst und Sport als Verantwortlichem erforderlichenfalls überprüft und dem oder den zuständigen Verantwortlichen gemäß § 280 Abs. 1 mitgeteilt werden können. Dieser kann beziehungsweise diese können aufgrund der Mitteilung im Rahmen seiner oder ihrer jeweiligen Verantwortlichkeit tätig werden und die personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten einer Klarstellung zuführen.

§ 280 Abs. 7 regelt die bereits bestehende Ermächtigung der Bundesministerin oder des Bundesministers für öffentlichen Dienst und Sport zur Verarbeitung, Übermittlung und Weiterverarbeitung von Adressdaten für Benachrichtigungen und Befragungen unter den angeführten Voraussetzungen sowie im Rahmen der vorzunehmenden Abwägung. Eine Verarbeitung, Übermittlung und Weiterverarbeitung gemäß dieser Bestimmung hat ausschließlich zum Zwecke der Benachrichtigung oder Befragung der betroffenen Personen zu erfolgen. Durch die zu berücksichtigenden Aspekte soll vor allem verhindert werden, dass zum Beispiel durch die Auswahl eines bestimmten Personenkreises für eine Benachrichtigung oder Befragung Rückschlüsse auf personenbezogene Daten oder besondere Kategorien personenbezogener Daten möglich sind.

In § 280a Abs. 1 wird ermöglicht, dass zusätzlich zur bereits bestehenden elektronischen Personenkennzeichnung auch ein bereichsspezifisches Personenkennzeichen gemäß § 9 des E-Government-Gesetzes – E-GovG, BGBl. I Nr. 10/2004, zum Zwecke der eindeutigen Identifikation der im § 280 Abs. 1 genannten betroffenen Personen im Beschäftigungskontext zur Anwendung kommen kann.

§ 280a Abs. 2 bis 5 enthält Bestimmungen zur Datenaufbewahrung im Rahmen der Personaldatenverarbeitung. Dem Grundsatz der Datenminimierung folgend ist es bei gemeinsam Verantwortlichen ausreichend, wenn die Aufbewahrungspflicht nur von einem Verantwortlichen wahrgenommen wird. Gesetzlich ist eine fünfzehnjährige Frist für personenbezogene Daten und besondere Kategorien personenbezogener Daten vorgesehen. Für Protokolldaten über lesende Zugriffe ist eine dreijährige Frist und für Protokolldaten über inhaltsändernde Zugriffe eine siebenjährige Frist vorgesehen. Diese Fristen ergeben sich aus einer Abwägung, die vor allem das Grundrecht auf Datenschutz, das Grundrecht auf Achtung des Privat- und Familienlebens, die Rechenschaftspflicht des jeweils Verantwortlichen, den Grundsatz der Integrität und Vertraulichkeit, den Grundsatz der Speicherbegrenzung, den Grundsatz der Datenminimierung, die Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, die verschiedenen Verjährungsfristen, das öffentliche Interesse, insbesondere im Hinblick auf den rechtskonformen Vollzug der Gesetze, die Erfüllung der Kernaufgaben des Staates, die Aufrechterhaltung und das ordnungsgemäße Funktionieren des Öffentlichen Dienstes sowie dessen Nachvollziehbarkeit, die bereits vorgefundene Wertung strafrechtlich geschützter Rechtsgüter sowie den Beschäftigungskontext berücksichtigt.

§ 280a Abs. 6 bestimmt, dass eine durch Gesetz oder Verordnung vorgesehene längere Aufbewahrungspflicht oder Archivierung den in § 280 Abs. 2 bis 5 vorgesehenen Aufbewahrungspflichten vorgeht. Etwaige längere Aufbewahrungspflichten sollen demnach nicht durch die Einführung einer Aufbewahrungspflicht gemäß § 280a verkürzt werden. Ebenso unberührt bleiben sollen die Löschpflicht von Strafregisterauskünften und die Löschpflicht gemäß § 79e Abs. 2a. Werden jedoch speziellere Fristen für Aufbewahrungspflichten durch den Verantwortlichen oder die gemeinsam Verantwortlichen mittels Verordnung vorgesehen, so gehen diese der jeweiligen Frist der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 vor. Die Fristen für Protokolldaten über lesende Zugriffe müssen jedoch mindestens ein Jahr und für Protokolldaten über inhaltsändernde Zugriffe

mindestens drei Jahre betragen, damit insbesondere die Rechte betroffener Personen nicht durch zu kurze Fristen beschränkt werden. Eine durch Gesetz oder Verordnung vorgesehene längere Frist einer Aufbewahrungspflicht oder Archivierung geht gemäß § 280 Abs. 6 auch einer durch Verordnung gemäß § 280a Abs. 7 festgesetzten kürzeren Frist vor. Gemeinsam Verantwortliche haben beim Erlassen einer Verordnung gemäß § 280a Abs. 7 das Einvernehmen herzustellen. Durch die Verordnungsermächtigung in § 280a Abs. 7 soll insbesondere den Grundsätzen der Speicherbegrenzung und Datenminimierung besonders Rechnung getragen werden können.

§ 280a Abs. 7 ermächtigt die Bundeskanzlerin oder den Bundeskanzler erforderlichenfalls zur nicht inhaltsändernden Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten, damit in Bezug auf die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verfahren rechtskonform gestaltet, Fehler behoben und die Datensicherheit gewährleistet werden können. Die Erforderlichkeit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten zu den genannten Zwecken ist eng auszulegen. Datensicherheit bezieht sich nicht nur auf den physischen Zugang zu den Personaldatensystemen, sondern bedeutet auch, dass sichergestellt wird, dass die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten nur berechtigten Personen ermöglichen und diese Daten nur berechtigten Personen zur Verfügung stehen. Personenbezogene Daten und besondere Kategorien personenbezogener Daten sind vor unrechtmäßigen Verarbeitungen, Übermittlungen oder Weiterverarbeitungen zu schützen, was insbesondere durch entsprechende Protokollierung zu erfolgen hat. Daher ist von dem oder den jeweils Verantwortlichen sicherzustellen, dass bestehende Protokolldaten nicht verändert werden können. Für Bereiche, in denen die Leiterinnen und Leiter der Zentralstellen jeweils mit der Bundeskanzlerin oder dem Bundeskanzler gemeinsam Verantwortliche sind, erfolgt gemäß § 280b Abs. 2 die Aufteilung der Pflichten unbeschadet der Stellung als gemeinsam Verantwortliche im Sinne der DSGVO durch Verordnung der Bundesregierung. Die Möglichkeit zur Festlegung der jeweiligen Aufgaben der Verantwortlichen durch Rechtsvorschriften der Mitgliedstaaten, denen die Verantwortlichen unterliegen, wird in Art. 26 Abs. 1 DSGVO eröffnet. Dadurch soll vor allem gewährleistet sein, dass betroffene Personen bei der Geltendmachung ihrer Rechte gemäß DSGVO hinsichtlich standardisierter IKT-Lösungen und IT-Verfahren des Personalmanagement des Bundes unabhängig davon, welche Konstellation gemeinsam Verantwortlicher vorliegt, vergleichbar behandelt werden.

§ 280b Abs. 1 wird aufgrund der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, angepasst.

Ein aufgrund der Verordnung der Bundesregierung gemäß § 280b Abs. 2 unzuständiger gemeinsam Verantwortlicher hat die betroffene Person gemäß § 280b Abs. 4 an den zuständigen gemeinsam Verantwortlichen zu verweisen. Die entsprechenden Informationen und damit auch die Information, wer zuständiger Verantwortlicher ist, haben auf direktem Weg von der Dienstbehörde oder Personalstelle an die betroffene Person zu ergehen. Direkt bedeutet, dass es dabei zu keiner Befassung von Zwischenvorgesetzten kommen soll. Es ist darauf zu achten, dass die Rechte Dritter nicht nachteilig beeinflusst werden, was insbesondere bei namentlicher Nennung Dritter der Fall sein kann. Die Übermittlung von Informationen kann bei Verständigung der betroffenen Person hiervon auch durch gesicherten Fernzugriff, also durch Abholung erfolgen. Es wird auf Art. 12 DSGVO verwiesen, der die transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der Betroffenen regelt. Für eine Verlängerung der Frist ist von Bedeutung, dass die betroffene Person vor Ablauf der Monatsfrist verständigt wird. Eine solche Verständigung hat jedenfalls eine Information über die Fristverlängerung und eine entsprechende Begründung zu enthalten.

In § 280b Abs. 5 bis 8 wird von der in Art. 23 DSGVO eröffneten Möglichkeit der Beschränkung der Pflichten und Rechte gemäß Art. 5, 12 bis 22 und 34 DSGVO Gebrauch gemacht. Dies erfolgt unter Beachtung des Wesensgehalts der Grundrechte und Grundfreiheiten. Dabei kommen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zur Anwendung. Derartige Beschränkungen von Rechten und Pflichten müssen darüber hinaus der Sicherstellung bestimmter Zwecke dienen, unter denen beispielsweise in Art. 23 Abs. 1 lit. e DSGVO der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“ genannt wird. Daneben können sich solche Beschränkungen beispielsweise auch auf Art. 23 Abs. 1 lit. f und h bis j DSGVO stützen. Die Verarbeitung, Übermittlung und Weiterverarbeitung von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten ist für den öffentlichen Dienst unerlässlich und liegt aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Aufrechterhaltung und dem

ordnungsgemäßen und rechtskonformen Funktionieren des öffentlichen Dienstes, insbesondere im Sinne einer Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, selbst im öffentlichen Interesse. Insbesondere ist es erforderlich, dass im öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung besteht und dass die Revisionssicherheit gewährleistet ist. Es ist daher erforderlich und sachgerecht, gewisse Beschränkungen der Rechte der betroffenen Personen vorzunehmen.

Ein Verantwortlicher ist nach der DSGVO zur Berichtigung, Aktualisierung oder Vervollständigung von personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten, die durch ihn verarbeitet werden, verpflichtet. Dies ergibt sich einerseits aus Art. 5 Abs. 1 lit. d DSGVO und andererseits aus dem Recht der betroffenen Person auf Berichtigung gemäß Art. 16 DSGVO. Der Rechtskraft fähige Erledigungen enthalten personenbezogene Daten und unter Umständen auch besondere Kategorien personenbezogener Daten, die grundsätzlich dem Recht auf beziehungsweise der Pflicht zur Berichtigung gemäß den Bestimmungen der DSGVO unterliegen. Da sich daraus ein Spannungsverhältnis zum allgemeinen Konzept der Rechtskraft beziehungsweise der Verjährung ergibt, ist eine Beschränkung des Grundsatzes der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO sowie des Rechtes auf Berichtigung gemäß Art. 16 DSGVO vorgesehen. § 280b Abs. 5 beschränkt den Grundsatz der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO sowie das Recht auf Berichtigung gemäß Art. 16 DSGVO bei unrichtigen oder unvollständigen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten insoweit, als einer Berichtigung die Rechtskraft oder die Verjährung entgegenstehen, oder wenn ein zumutbarer Rechtsweg besteht oder bestand. Dies dient nicht nur dem Schutz des jeweils vorgesehenen Verfahrens, sondern stellt insbesondere klar, dass das Recht auf Berichtigung auch im Anwendungsbereich der §§ 280 ff nicht der Umgehung anderer rechtlicher Vorschriften oder eines durch den Gesetzgeber vorgesehenen Rechtsweges dient. Dass eine nicht inhaltsändernde Stellungnahme abgegeben werden kann, bedeutet, dass im Sinne einer Vervollständigung oder ergänzenden Erklärung zwar von den personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten abweichende Inhalte angeführt werden können, diese Inhalte der personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten gemäß § 280 Abs. 1 aber aufgrund der Stellungnahme nicht geändert werden dürfen. Die Wahrung der Rechtssicherheit und Rechtsbeständigkeit stellt ein wichtiges Ziel des allgemeinen öffentlichen Interesses dar und daher ist eine Beschränkung im Ausmaß des § 280b Abs. 5 von Art. 23 Abs. 1 lit. e DSGVO gedeckt.

§ 280b Abs. 6 stellt klar, dass für zulässig verarbeitete Daten das Recht auf Löschung gemäß Art. 17 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung ausgeschlossen ist. Eine solche Möglichkeit besteht gemäß Art. 17 Abs. 3 DSGVO zur Erfüllung einer rechtlichen Verpflichtung, wie beispielsweise einer Aufbewahrungspflicht, die die Verarbeitung nach dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Zur Aufrechterhaltung des öffentlichen Dienstes und der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten von betroffenen Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten bis zum Ablauf der durch Gesetz oder durch Verordnung bestimmten Frist der Aufbewahrungspflicht erforderlich. Auf Art. 17 Abs. 3 lit. d und e DSGVO wird außerdem hingewiesen. Macht eine betroffene Person glaubhaft, dass die Aufbewahrung ihrer personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten sie erheblich in ihren Rechten beeinträchtigt, so kann auf Antrag der betroffenen Person für die verbleibende Dauer der Aufbewahrungspflicht eine Speicherung ohne Aufbereitung vorgesehen werden, wenn für diesen Zeitraum keine weitere Verarbeitung, Übermittlung oder Weiterverarbeitung vorgesehen ist.

§ 280b Abs. 7 regelt eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Die Überprüfung der Richtigkeit der personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der betroffenen Person soll nicht dazu führen, dass in den standardisierten IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verarbeitung, Übermittlung und Weiterverarbeitung einzuschränken wäre, was beispielsweise ein momentanes Anhalten der Vorrückung oder eine nicht zeitgerechte Anweisung des zustehenden Bezuges zur Folge haben kann. Alleine das Bestehen dieser möglichen Folgen aufgrund der integrierten Datenverarbeitungssysteme würde neben der Verursachung eines beträchtlichen Verwaltungsaufwandes für viele betroffene Personen die Geltendmachung ihrer Rechte gemäß DSGVO erschweren oder faktisch unmöglich machen, weswegen für den Anwendungsbereich der §§ 280 ff eine Beschränkung des Rechtes auf Einschränkung

der Verarbeitung im erforderlichen Ausmaß sachgerecht ist. Gleiches gilt für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung ist auch im Lichte des wichtigen wirtschaftlichen und finanziellen Interesses des Staates, beispielsweise im Haushalts- und Steuerbereich, erforderlich und sachgerecht im Sinne des Art. 23 Abs. 1 lit. e DSGVO, da etwa die rechtskonforme Abführung von Beiträgen zur Sozialversicherung und der Lohnsteuer, der rechtskonforme Vollzug der Personaladministration, die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung und die Revisionssicherheit wichtige Ziele des allgemeinen öffentlichen Interesses darstellen, deren Schutz die Beschränkung gemäß § 280 Abs. 7 rechtfertigt.

Aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Verarbeitung der personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der Personen gemäß § 280 Abs. 1 ist es erforderlich und sachgerecht, das Recht auf Widerspruch gemäß Art. 21 DSGVO in § 280b Abs. 8 für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung auszuschließen, sofern die betroffene Person nicht Gründe nachweisen kann, die sich aus ihrer besonderen Situation ergeben und die die Ziele der Beschränkung des Rechtes auf Widerspruch überwiegen. Die Erforderlichkeit und Sachlichkeit dieser Beschränkung ergibt sich aus dem überwiegenden, berechtigten öffentlichen Interesse an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des öffentlichen Dienstes, konkret dem rechtskonformen Vollzug der Personaladministration, dem rechtskonformen Abführen von Beiträgen, beispielsweise zur Sozialversicherung und der Lohnsteuer sowie der Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit. Insbesondere ist es erforderlich, dass im öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung besteht und dass die Revisionssicherheit gewährleistet ist. Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 1 erfolgen ausschließlich zu in § 280 Abs. 2 genannten Zwecken, sofern dies erforderlich ist. Auch für die weiteren Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß den §§ 280 und 280a Abs. 1 und 7 besteht ein überwiegendes, berechtigtes öffentliches Interesse, wobei auch auf Art. 21 Abs. 6 DSGVO hingewiesen wird. Darüber hinaus würde für den Fall, dass eine betroffene Person ihr Recht auf Widerspruch geltend macht, nicht zuletzt aufgrund der integrierten Datenverarbeitungssysteme mindestens eine weitere Verarbeitung, Übermittlung und Weiterverarbeitung erforderlich werden, was dem grundsätzlichen Anliegen der betroffenen Person zuwiderlaufen würde. Es wird daher eine sachgerechte und erforderliche Beschränkung des Rechtes auf Widerspruch gemäß Art. 21 DSGVO im Sinne des Art. 23 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung vorgeschlagen, sofern nicht eine beschriebene besondere Situation vorliegt. In Fällen, in denen das Widerspruchsrecht nicht gemäß § 280b Abs. 8 eingeschränkt ist, kann sich direkt aus Art. 21 Abs. 1 letzter Satz und Abs. 6 letzter Satz DSGVO ergeben, dass trotz Widerspruchs eine Verarbeitung, Übermittlung oder Weiterverarbeitung personenbezogener Daten zulässig ist.

Die bezughabende Datenschutz-Folgenabschätzung findet sich als **Anlage** im Anschluss an die Erläuterungen.

Zu Art. 16 (Änderung des Gehaltsgesetzes 1956)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 16 Z 1 (§ 171 GehG):

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in den §§ 280 bis 280b BDG 1979 kann § 171 entfallen.

Zu Art. 17 (Änderung des Vertragsbedienstetengesetzes 1948)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 17 Z 1 und 3 (Inhaltsverzeichnis, § 96 und § 96a VBG):

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in den §§ 280 bis 280b BDG 1979 kann § 96 entfallen.

In § 280a Abs. 1 BDG 1979 erfolgt eine Anpassung des Personenkreises an § 280 Abs. 1 BDG 1979, weswegen § 96a entfallen kann.

Zu Art. 17 Z 2 (§ 3 Abs. 4 VBG):

Auf die Erläuterungen zu § 204 Abs. 7 BDG 1979 wird verwiesen.

Zu Art. 18 (Änderung des Richter- und Staatsanwaltschaftsdienstgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 18 Z 1 (Artikel VI RStDG):

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in den §§ 280 bis 280b BDG 1979 kann Artikel VI entfallen.

Zu Art. 18 Z 2 (§ 3 Abs. 1 RStDG):

Auf die Erläuterungen zu § 204 Abs. 7 BDG 1979 wird verwiesen.

Zu Art. 19 (Änderung des Landeslehrer-Dienstrechtsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 2 B-VG.

Zu Art. 19 Z 1 (§ 6 Abs. 5 LDG 1984):

Auf die Erläuterungen zu § 204 Abs. 7 BDG 1979 wird verwiesen.

Zu Art. 19 Z 2 (§ 119a LDG 1984):

Die Ermächtigung für die Länder bestimmte Daten zu verarbeiten, bedarf einer Anpassung an die DSGVO.

Neben der Verarbeitung, Übermittlung und Weiterverarbeitung von Daten für Landeslehrpersonen gemäß § 1 und Landesvertragslehrpersonen gemäß § 1 LVG erstreckt sich die gegenständliche Ermächtigung auch einerseits auf Daten von Bundeslehrpersonen gemäß § 1 Abs. 1 BDG 1979 sowie § 1 Abs. 1 VBG, um eine Verarbeitung von Daten von Bundeslehrpersonen, die an Pflichtschulen mitverwendet werden, sicherzustellen und andererseits auf in einem Dienstverhältnis zu einem privaten Rechtsträger stehende Lehrpersonen (Lehrpersonen nach § 19 Abs. 3 PrivSchG sowie kirchlich bestellte Religionslehrpersonen), da für die Lehrpersonen nach § 19 Abs. 3 PrivSchG die Besoldung durch die Länder erfolgen muss.

Im Übrigen wird auf die Ausführungen zu §§ 280, 280a und 280b BDG 1979 verwiesen, insoweit die jeweiligen Absätze in § 119a für anwendbar erklärt werden.

Zu Art. 20 (Änderung des Land- und forstwirtschaftlichen Landeslehrer-Dienstrechtsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14a Abs. 3 B-VG.

Zu Art. 20 Z 1 (§ 6 Abs. 5 LLDG 1985):

Auf die Erläuterungen zu § 204 Abs. 7 BDG 1979 wird verwiesen.

Zu Art. 20 Z 2 und 3 (§ 119h und § 124a LLDG 1985):

Bezüglich § 119h wird, insoweit die jeweiligen Absätze in § 119h für anwendbar erklärt werden, auf die Ausführungen zu §§ 280, 280a und 280b BDG 1979 verwiesen.

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in § 119h kann § 124a entfallen.

Zu Art. 21 (Änderung des Bundes-Gleichbehandlungsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 21 Z 1 und 2 (§ 12 Abs. 2 und § 25 Abs. 6 B-GlBG):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 22 (Änderung des Pensionsgesetzes 1965)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 22 Z 1 bis 9 (§ 1a Abs. 1 bis 3, Überschrift zu § 101, § 101 Abs. 1 und 2, § 102 und § 105 Abs. 5 PG 1965):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 23 (Änderung des Bundestheaterpensionsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 6 B-VG (Zivilrechtswesen).

Zu Art. 23 Z 1 bis 8 (§ 1a Abs. 1 bis 3, Überschrift zu § 21, § 21 Abs. 1 und 2 und § 21a BThPG):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 24 (Änderung des Bundesbahn-Pensionsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 6 B-VG (Zivilrechtswesen).

Zu Art. 24 Z 1 bis 3 und Z 5 bis 9 (§ 1a Abs. 1 bis 3, Überschrift zu § 68, § 68 Abs. 1 und 2 und § 69 BB-PG):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 25 (Änderung des Bundespensionsamtübertragungs-Gesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 4 B-VG.

Zu Art. 25 Z 1 und 2 (§ 5 BPAÜG):

Die Versicherungsanstalt öffentlich Bediensteter (BVA) vollzieht seit 2007 im übertragenen Wirkungsbereich der Bundesministerin oder des Bundesministers für Finanzen die pensionsrechtlichen Angelegenheiten der Beamtinnen und Beamten des Bundes; die Zuständigkeit der Versicherungsanstalt wurde aus sachlichen Erwägungen zwischenzeitig in den Bereichen der Ruhe- und Versorgungsbezüge, des Pflegegeldes und der Heimopferrenten erweitert. Die Versicherungsanstalt verwendet in den genannten Aufgabenbereichen die IT-Verfahren des Bundes, insbesondere die Bundesbesoldung als Datenquelle der Aktivbesoldung für die Bemessung von Ruhestands- und Hinterbliebenenansprüchen sowie für die laufende Verrechnung und Auszahlung der Leistungen (vgl. § 4 Haushaltsrechtliche Anordnungsbefugnisse) und den ELAK; die Bundesrechenzentrum Gesellschaft fungiert als EDV-Dienstleister. Die Verwendung der IT-Verfahren des Bundes in den übertragenen Wirkungsbereichen wurde zuletzt mit einer Änderung des § 5 Abs. 2 klargestellt (Art. 15 der Dienstrechts-Novelle 2015, BGBl. I Nr. 65/2015); dabei wurde bereits nicht nur auf die Vollzugsbereiche des BPAÜG sondern auch an die zwischenzeitigen Erweiterungen der Zuständigkeiten angeknüpft („…bei der Vollziehung weiterer ihr in entsprechender Anwendung dieses Bundesgesetzes übertragenen Aufgaben…“). Die nun angezeigte Aufnahme der datenschutzrechtlichen Bestimmungen steht aufgrund der Datenverarbeitung in engem Zusammenhang mit der angesprochenen Regelung der IT-Verfahren. Die Regelungen zur Datenverarbeitung für die Ressorts können somit aus inhaltlicher Sicht mit den entsprechenden Anpassungen für die von der BVA betreuten Personengruppen sowie die Zwecke der Datenverarbeitungen zur Anwendung gelangen. Die Benennung der oder des Datenschutzbeauftragten erfolgt durch die BVA in Wahrnehmung der gemeinsamen Verantwortlichkeit mit der Bundesministerin oder dem Bundesminister für Finanzen nach Art. 37 DSGVO.

Zu Art. 26 (Änderung des Bundes-Personalvertretungsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

Zu Art. 26 Z 1 bis 9 (§ 9 Abs. 2 lit. f, n und o sowie Abs. 3 lit. i, n und o, § 10a Abs. 1 und 3 und § 14 Abs. 3 PVG):

Es erfolgen terminologische Anpassungen an das neue Datenschutzrecht.

Zu Art. 27 (Änderung des Rechtspraktikantengesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 6 B-VG (Zivil- und Strafrechtswesen, Justizpflege, Angelegenheiten der Notare, der Rechtsanwälte sowie verwandter Berufe).

Zu Art. 27 Z 1 (§ 2 Abs. 3a RPG):

Auf die Erläuterungen zu § 204 Abs. 7 BDG 1979 wird verwiesen.

Zu Art. 27 Z 2 (§ 26a RPG):

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in den §§ 280 bis 280b BDG 1979 kann § 26a RPG entfallen.

Zum 3. Hauptstück (Arbeit, Soziales und Konsumentenschutz)

Allgemeines:

Im Zusammenhang mit dem mit 25. Mai 2018 wirksam werdenden Datenschutzregime müssen insbesondere die datenschutzrechtlichen Begrifflichkeiten an die neuen Definitionen der DSGVO angepasst werden. Weiters sieht die DSGVO manchmal Regelungsspielräume („Öffnungsklauseln“) für die nationale Gesetzgebung vor, die unter anderem auch dazu genutzt werden können, Regelungen im Bereich des Datenschutzes zu konkretisieren (so etwa hinsichtlich Aufbewahrungsfristen).

Der vorliegende Entwurf enthält die erforderlichen Anpassungen für die Bundesgesetze im Wirkungsbereich des Bundesministeriums für Arbeit, Soziales, Gesundheit und Konsumentenschutz, wobei jedoch für die Anpassungen im Bereich der gesetzlichen Sozialversicherung und im Bereich Gesundheit einem gesonderten Vorhaben vorbehalten ist.

Zum 1#. Abschnitt (Konsumentenschutz)

Zu Art. 28 (Änderung des Alternative-Streitbeilegung-Gesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 6 B-VG.

Zu Art. 28 Z 1 (§ 8 Abs. 2):

Auf Grund der in der DSGVO ohnehin enthaltenen und unmittelbar anzuwendenden Bestimmungen können die entsprechenden Bestimmungen im AStG entfallen.

Zu Art. 29 (Änderung des Produktsicherheitsgesetzes 2004)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 7, 8, 9, 10 und 12 B-VG.

Zu Art. 29 Z 1 (§ 8 Abs. 4 PSG 2004):

Die Verordnung (EWG) Nr. 339/93 wurde aufgehoben und ihre Bestimmungen in die Verordnung (EG) Nr. 765/2008 integriert; der Verweis wird daher entsprechend angepasst. Zudem wird konkretisiert, zu welchem Zweck eine Datenübermittlung stattfinden darf.

Zu Art. 29 Z 2 (§ 9 PSG 2004):

Der dritte Satz in § 9 PSG 2004 kann auf Grund der in der DSGVO enthaltenen und unmittelbar anzuwendenden Bestimmungen entfallen.

Zu Art. 29 Z 3 und 4 (§ 10 PSG 2004):

In Abs. 1 wird die exemplarische Anführung europäischer Produktsicherheit-Meldeverfahren auf die Verfahren in der Verordnung (EG) Nr. 765/2008 erweitert.

Abs. 2 entfällt auf Grund der entsprechenden und unmittelbar anzuwendenden Bestimmungen in der DSGVO; der Abs. 3 wird entsprechend angepasst.

Zum 2. Abschnitt (Soziales)

Zu Art. 30 (Änderung des Behinderteneinstellungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. I Abs. 2 des Bundesgesetzes vom 27. September 1988, BGBl. Nr. 721.

Zu Art. 30 Z 1 und 2 (§§ 16 und 19a BEinstG):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 31 (Änderung des Bundesbehindertengesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 17 B-VG.

Zu Art. 31 Z 1 (§ 13c Abs. 5 BBG):

§ 13a BBG und die nachfolgenden Bestimmungen regeln die Stellung und die gesetzlichen Aufgaben des Behindertenanwalts. Zur ordnungsgemäßen Erfüllung der gesetzlichen Aufgaben ist es für den Behindertenanwalt notwendig, personenbezogene Daten zu verarbeiten. Daher ist insbesondere im Lichte des Art. 6 Abs. 1 lit. c und e DSGVO ein datenschutzrechtlicher Bedarf nach einer gesetzlichen Ermächtigung zur Verarbeitung personenbezogener Daten durch den Behindertenanwalt gegeben. Sowohl das Datum Grad der Behinderung als auch allfällige Daten aus den medizinischen Gutachten sollen dazu dienen, bei der Unterstützung von hilfesuchenden Menschen mit Behinderung möglichst konkret die Problemlage zu umreißen.

Zu Art. 31 Z 2 bis 13 (§ 13d Abs. 5, § 30, § 52 und § 53 BBG):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 32 (Änderung des Bundes-Behindertengleichstellungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 6 und 11 B-VG.

Zu Art. 32 Z 1 (§ 16):

§ 16a Bundes-Behindertengleichstellungsgesetz (BGStG) soll die gesetzliche Ermächtigung für das Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz sowie das Bundesamt für Soziales und Behindertenwesen darstellen, die für die Vollziehung erforderlichen personenbezogenen Daten zu verarbeiten. Durch die Aufzählung der Datenarten wird den Erfordernissen der Datenschutz-Grundverordnung und des Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 Rechnung getragen. Da für Beratungen und Durchführung von Schlichtungsverfahren nach dem BGStG auch bestimmte personenbezogene Daten der beteiligten Personen benötigt werden, sollen das Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz und das Bundesamt für Soziales und Behindertenwesen ermächtigt werden, auch diese personenbezogenen Daten zu verarbeiten.

Zu Art. 33 (Änderung des Bundespflegegeldgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG und Art. 102 Abs. 2 B-VG.

Zu Art. 33 Z 1 (§ 21a Abs. 5, 6 und 7 BPGG):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

§ 21a Abs. 5 und 6 soll die gesetzliche Ermächtigung für das Bundesamt für Soziales und Behindertenwesen darstellen, die für die Vollziehung erforderlichen personenbezogenen Daten zu verarbeiten. Durch die Aufzählung der Datenarten wird den Erfordernissen der Datenschutz-Grundverordnung und des Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 Rechnung getragen. Da für die Gewährung einer Zuwendung aus dem Unterstützungsfonds für Menschen mit Behinderung auch bestimmte personenbezogene Daten der pflegebedürftigen Person (z. B. Pflegegeldstufe) benötigt werden, soll das Bundesamt für Soziales und Behindertenwesen ermächtigt werden, auch diese personenbezogenen Daten zu verarbeiten.

Im Abs. 7 soll das Bundesamt für Soziales und Behindertenwesen aus verwaltungsökonomischen Gründen ermächtigt werden, die personenbezogenen Daten der pflegebedürftigen Person im Einzelfall aus der Anwendung Pflegegeldinformation – PFIF des Hauptverbandes der österreichischen Sozialversicherungsträger abzufragen.

Zu Art. 33 Z 2, 3, 4 und 6 (§ 21b Abs. 7, 8, 10 und 12):

Das gesamte Förderungsverfahren zu § 21b BPGG wird für Neufälle ab dem ersten Quartal 2018 vollelektronisch geführt werden. Es sollen sowohl die in der bislang geltenden Fassung des § 21b Abs. 7 BPGG genannten Daten sowie die im Rahmen des gegenständlichen Entwurfes ergänzten Daten sodann automationsunterstützt im Rahmen einer beim Sozialministeriumservice betriebenen IT-Anwendung (Dateisystem im Sinne des Art. 4. Z 6 DSGVO) verarbeitet werden.

Die vorgeschlagenen legistischen Anpassungen sollen in Entsprechung der Datenschutz-Grundverordnung, insbesondere unter Berücksichtigung deren Art. 5, 6, 9 und 32, erfolgen. Die Regelungen der § 21b Abs. 10 erster Satz und Abs. 12 können auf Grund des Anwendungsvorranges des Art. 32 der Datenschutz-Grundverordnung entfallen.

Bei der Änderung in § 21b Abs. 7 Z 3 handelt es sich um eine redaktionelle Anpassung.

Zu Art. 33 Z 7 bis 10, 14 bis 16 und 18 (§§ 21e, 33 und 45 BPGG):

Die Begriffe „Daten“, „Dienstleister“ und „Verwendung“ werden durch die entsprechenden Begriffe der Datenschutz-Grundverordnung ersetzt.

Zu Art. 33 Z 11 bis 13 (§ 32 BPGG):

Der Begriff der Datenverarbeitung in § 32 soll die in Art. 4 Z 2 der Datenschutz-Grundverordnung genannten Verarbeitungsvorgänge ohne die Offenlegung durch Übermittlung umfassen.

Zu Art. 33 Z 17 (§ 33a Abs. 3 und 4 BPGG):

Durch die im § 33a Abs. 2 BPGG normierten Angehörigengespräche sollen Beiträge zur Reduzierung von psychischen Belastungen geleistet, individuelle Handlungsoptionen anhand von Ressourcen aufgezeigt, der Zugang zu relevanten Unterstützungsangeboten erleichtert und Ressourcen von pflegenden Angehörigen in Belastungssituationen erfasst werden.

Jenen Angehörigen, welche beim Hausbesuch durch eine diplomierte Pflegefachkraft im Rahmen der Qualitätssicherung in der häuslichen Pflege zumindest eine psychische Belastung angegeben haben, wird das Angehörigengespräch angeboten. Überdies kann das Angehörigengespräch auch auf Wunsch der Betroffenen erfolgen. Durchgeführt wird das Angehörigengespräch von Psychologen und Psychologinnen. Die Organisation der Gespräche erfolgt durch das Kompetenzzentrum bei der Sozialversicherungsanstalt der Bauern.

Durch den neuen Abs. 3 soll nunmehr die datenschutzrechtliche Ermächtigung geschaffen werden, dass das Kompetenzzentrum bei der Sozialversicherungsanstalt der Bauern die im Rahmen der Angehörigengespräche erhobenen personenbezogenen Daten automationsunterstützt verarbeiten kann. Durch die Aufzählung der Datenarten wird den Erfordernissen der Datenschutz-Grundverordnung und des Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 Rechnung getragen.

Im Abs. 4 soll normiert werden, dass die personenbezogenen Daten an die Anwendung Pflegegeldinformation – PFIF, die beim Hauptverband der österreichischen Sozialversicherungsträger nach den Weisungen des Sozialministeriums geführt wird, von der Sozialversicherungsanstalt der Bauern zu übermitteln sind. Dadurch besteht die Möglichkeit, durch Selektion von Personenkreisen gezielt weitere Maßnahmen zur Qualitätssicherung anzubieten und die Situation pflegender Angehöriger zu verbessern.

Überdies ist dadurch auch die Erstellung statistischer Auswertungen möglich.

Zu Art. 34 (Änderung des Ehrengaben- und Hilfsfondsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 34 Z 1 und 2 (§§ 13 dritter Satz und 14 Abs. 2):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 35 (Änderung des Heeresentschädigungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 35 Z 1 bis 6 (§§ 5 und 6 HEG):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 36 (Änderung des Heimopferrentengesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 36 Z 2 und 4 (§§ 11 und 12 HOG):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 36 Z 3 (§ 11 Abs. 4 Z 2 lit. d und Z 5 HOG):

Die in § 11 Abs. 4 Z 2 lit. d und Z 5 genannten, personenbezogenen Daten betreffend „die näheren Umstände und zugefügten Verletzungen“ bzw. „Arbeitsfähigkeit“ sollen nur die in der taxativen Aufzählung des Art. 9 der Datenschutz-Grundverordnung genannten Gesundheitsdaten als besondere Kategorie personenbezogener Daten umfassen.

Zu Art. 37 (Änderung des Impfschadengesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 37 Z 1 und 2 (§ 3 Abs. 3):

Der Verweis auf das bis zum 30. Juni 2016 in Geltung stehende Heeresversorgungsgesetz soll durch einen Verweis auf die aktuellen Bestimmungen des Heeresentschädigungsgesetzes ersetzt werden.

Zu Art. 38 (Änderung des Kriegsgefangenenentschädigungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 38 Z 1 bis 5 (§§ 17 und 18):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 39 (Änderung des Kriegsopferversorgungsgesetzes 1957)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 39 Z 1 bis 3 (§§ 91a, 91b und 93):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 40 (Änderung des Sozialministeriumservicegesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 16 B-VG.

Zu Art. 40 Z 1 bis 8 (§ 2a Abs. 1 bis 5):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zu Art. 41 (Änderung des Verbrechensopfergesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 41 Z 1 und 2 (§ 9 Abs. 5 und § 9c Abs. 2):

Der Begriff „Daten“ soll durch den in Art. 4 Z 1 der Datenschutz-Grundverordnung festgelegten Ausdruck „personenbezogene Daten“ ersetzt werden.

Zum 3. Abschnitt (Arbeit)

Zu Art. 42 (Änderung des Arbeitsmarktservicegesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 42 Z 1 (§ 25 AMSG):

Das Arbeitsmarktservice Österreich (AMS) ist als Dienstleistungsunternehmen des öffentlichen Rechts eingerichtet (§ 1 AMSG) und hinsichtlich der Datenverarbeitung Verantwortlicher des öffentlichen Bereiches gemäß § 26 Abs. 1 Z 1 DSG (idF BGBl. I Nr. 120/2017). Dem Arbeitsmarktservice wurde die Erfüllung einer Vielzahl an öffentlichen, gesetzlich vorgegebenen Aufgaben sowie auch die Erbringung der dafür erforderlichen Leistungen übertragen. Kernaufgaben sind die Versorgung der Wirtschaft mit entsprechend ausgebildeten Arbeitskräften, die Sicherung der Beschäftigung arbeitsuchender Personen durch Vermittlungstätigkeiten und die Sicherung der Existenz arbeitsloser Personen während der Jobsuche (§ 29 AMSG). Für die Erfüllung dieser Kernaufgaben sind im Umfeld weitere umfangreiche Leistungen zu erbringen. Als Beispiel sind Schulungsmaßnahmen für arbeitslose Personen, die Sicherstellung von Ausbildungsmöglichkeiten für Jugendliche, die Förderung gesundheitlich beeinträchtigter Personen, die Prüfung des Arbeitsmarktzugangs ausländischer Arbeitskräfte und die Arbeitsmarktbeobachtung sowie diesbezügliche wissenschaftliche und statistische Untersuchungen zu nennen. Die dem AMS gesetzlich übertragenen Aufgaben finden sich insbesondere im AMSG, im Arbeitsmarktpolitik-Finanzierungsgesetz (AMPFG), im Arbeitsmarktförderungsgesetz (AMFG), im Arbeitslosenversicherungsgesetz 1977 (AlVG), im Ausländerbeschäftigungsgesetz (AuslBG) und im Überbrückungshilfengesetz (ÜHG), aber auch im Arbeit-und-Gesundheit-Gesetz (AGG), BGBl. I Nr. 111/2010, im Ausbildungspflichtgesetz (APflG), BGBl. I Nr. 62/2016, und im Integrationsjahrgesetz (IJG), BGBl. I Nr. 75/2017. In diesen Gesetzesmaterien ist dem AMS regelmäßig die Mitwirkung an Maßnahmen anderer Behörden oder Einrichtungen aufgetragen, die zur nachhaltigen (Wieder-)Eingliederung von Personen in den Arbeitsmarkt erforderlich sind.

Für die Erfüllung der Vielzahl an gesetzlich übertragenen Aufgaben bedarf es zwingend einer entsprechend umfangreichen Verarbeitung von Datenarten, sowohl von betroffenen Personen als auch von Betrieben (Arbeitgebern). § 25 AMSG ermöglicht dem AMS für die Erfüllung der gesetzlichen Aufgaben aus diesem Grund eine umfangreiche Verarbeitung von Datenarten. Daneben bestehen für das AMS in den oben genannten Materiengesetzen gleichfalls spezifische gesetzliche Ermächtigungen zur Datenverarbeitung (vgl. zB § 69 AlVG, §§ 27 und 27a AuslBG, § 6 AMFG sowie § 7 AGG), die überwiegend die gegenseitige Zusammenarbeit sowie Rechts- und Amtshilfe konkretisieren.

§ 25 AMSG soll im Hinblick auf das Inkrafttreten der Datenschutz-Grundverordnung mit 25. Mai 2018 um Bestimmungen betreffend Aufbewahrungsfristen von Daten, Datensicherheitsmaßnahmen und das Erfordernis einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) ergänzt sowie an die Begrifflichkeiten der DSGVO angepasst werden.

Zu Art. 42 Z 1 (§ 25 Abs. 1 bis 8 AMSG):

In Abs. 7 werden das Sozialministeriumservice und Einrichtungen, denen Aufgaben des Arbeitsmarktservice übertragen sind, als Empfänger von Gesundheitsdaten ergänzt, um die in § 7 Abs. 2 AGG bereits bestehende gesetzliche Ermächtigung systematisch auch im AMSG abzubilden als auch die Möglichkeit der Übermittlung der Daten bei Inanspruchnahme von Dienstleistern durch das AMS klarzustellen.

Der Wortlaut „ausschließlich“ in Abs. 7 soll zur Klarstellung entfallen, da der Begriff „Arbeitsfähigkeit“ nicht eng im Sinne „ja/nein“ auszulegen ist, sondern auch Einschränkungen der Arbeitsfähigkeit im Sinne teilweiser oder temporärer gesundheitlicher Einschränkungen umfasst, wie dies etwa bei Rehageldbezieher/innen oder Teilnehmerinnen und Teilnehmern am Informations-, Beratungs- und Unterstützungsangebot nach dem AGG der Fall ist.

Die Protokollierungspflichten sind neu in Abs. 10 geregelt und sollen daher in Abs. 7 entfallen. Im Übrigen werden in den Abs. 1 bis 8 die Begrifflichkeiten an jene der DSGVO angepasst.

Zu Art. 42 Z 1 (§ 25 Abs. 9 AMSG):

Abs. 9 regelt die Aufbewahrungsfristen der gemäß Abs. 1 verarbeiteten Daten und soll sicherstellen, dass die Daten entsprechend dem Bedarf der Behörde ausreichend lange verarbeitet werden dürfen. Die Aufbewahrungsfrist wird generell mit sieben Jahren nach Beendigung des Geschäftsfalles festgelegt. Als Beendigung eines Geschäftsfalles ist zB die Abmeldung von der Vormerkung als arbeitsuchend, das Ende der Geltungsdauer einer Beschäftigungsbewilligung oder das Ende eines Stellensuchauftrages zu verstehen.

Werden lang zurückliegende Daten eines Leistungsbezuges oder einer Vormerkung für einen späteren Leistungsantrag wiederum benötigt, können diese Daten im Wege der beim Hauptverband der Sozialversicherungsträger bestehenden Versicherungsdatei übernommen werden.

Längere, über sieben Jahre hinausgehende Aufbewahrungsfristen können sich für Zwecke der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder aus anderen Rechtsvorschriften ergeben. So sieht beispielsweise § 24 Abs. 2 Z 4 der Allgemeinen Rahmenrichtlinien für die Gewährung von Förderungen aus Bundesmitteln (ARR 2014), BGBl. II Nr. 208/2014, eine zehnjährige Aufbewahrungsfrist von Unterlagen für gewährte Förderungen vor bzw. darüber hinaus, wenn dies unionsrechtliche Vorschriften vorsehen.

Längere Aufbewahrungsfristen ergeben sich in einer auslaufenden Übergangsphase auch für Bezugs- und Vormerkzeiträume von ehemals arbeitslosen Personen, die Zeiträume vor der Speicherung pensionsrelevanter Bezugs- und Vormerkdaten arbeitsloser Personen in der Versicherungsdatei beim Hauptverband der Sozialversicherungsträger (Zeiten vor 1976) betreffen und nicht aus dieser übernommen werden können, aber für die Beurteilung und Berechnung eines neuen Anspruches erforderlich sind. Diese Daten sind nicht sieben Jahre nach Beendigung des Geschäftsfalles zu löschen, wenn sie noch für die Geltendmachung von Rechtsansprüchen benötigt werden können.

Aus wirtschaftlichen und technischen Gründen soll die Löschung von Daten an wenigen Terminen im Jahre vorgenommen werden. Diese Anordnung soll punktuelles Vorgehen im Falle von Anträgen von betroffenen Personen vermeiden, die zu einem unwirtschaftlichen und technisch schwer lösbaren Vorgehen führen würden.

Zu Art. 42 Z 1 (§ 25 Abs. 10 und 11 AMSG):

Gemäß Art. 35 Abs. 1 der DSGVO haben Verantwortliche eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Datenverarbeitung **neue Technologien** verwendet oder **Art, Umfang, Umstände und Zweck der Verarbeitung** voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Beispielhaft sind die Verarbeitungen aufgezählt, bei denen

a) sich eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen einschließlich Profiling samt darauf folgender Entscheidungen auf eine automatisierte Verarbeitung gründet,

b) eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (wie Gesundheitsdaten oder Daten über strafrechtliche Verurteilungen) oder

c) eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

Für die Datenverarbeitungen des AMS spielt der **Umfang der verarbeiteten Daten**, hinsichtlich der Anzahl der betroffenen Personen wie auch des Ausmaßes der je betroffener Person verarbeiteten Datenarten für die Frage der Folgenabschätzung die wesentliche Rolle.

Wie schon einleitend dargestellt, muss das AMS aufgrund der umfangreichen gesetzlich übertragenen Aufgaben die dafür erforderlichen Datenarten verarbeiten, sprich erheben, erfassen, ordnen, sichern, speichern, bei Änderungen richtigstellen, auslesen, abfragen, abgleichen, verknüpfen, anderen Behörden oder SV-Trägern bereitstellen bzw. übermitteln, löschen sowie auch indirekt personenbezogen (pseudonymisiert) weiterverarbeiten.

Die Datenarten sind in § 25 AMSG aufgezählt, ergänzt um Bestimmungen in anderen Materiengesetzen (wie AlVG, AuslBG und AMFG). Soweit das Arbeitsmarktservice an der Erfüllung gesetzlicher Aufgaben anderer Behörden mitwirkt, finden sich weitere Bestimmungen auch im AGG, APflG und IJG. Für die Kernaufgaben des Arbeitsmarktservice sind stets Stammdaten von Arbeitsuchenden wie auch Unternehmen, die Arbeit anbieten, zu verarbeiten. Dies schließt die jeweiligen Kenntnisse und Fähigkeiten (schulische und berufliche Ausbildung) der Arbeitsuchenden mit ein sowie auch das Anforderungsprofil offener Stellen, die von Unternehmen bekannt gegeben werden. Die Mitarbeiterinnen und Mitarbeiter des AMS erfassen die erforderlichen Daten Arbeitsuchender, sowohl hinsichtlich der Vermittlungsmöglichkeiten von Jobs als auch hinsichtlich der Voraussetzungen für die Anweisung einer Unterstützungsleistung (wie Arbeitslosengeld, Notstandshilfe). Dies geschieht durch Anträge der betroffenen Personen mittels Papier oder elektronischem Antrag. Mit der betroffenen Person wird in weiterer Folge eine möglichst konkrete Betreuungsvereinbarung geschlossen, die eine nachhaltige Integration in den Arbeitsmarkt ermöglichen soll. Bei Leistungen an beschäftigte Personen (Weiterbildungsgeld, Bildungsteilzeitgeld) werden die dafür erforderlichen Datenarten erhoben und gespeichert. Einer laufenden Betreuung während der Weiterbildungsmaßnahmen bedarf es hier nicht.

Je nach Zuständigkeit der regionalen Geschäftsstellen (vgl. Arbeitsmarktsprengelverordnung) dürfen (und können) nur diese die Erfassungen oder Änderungen bei den in ihrem Sprengel wohnenden Arbeitsuchenden durchführen. Die EDV spiegelt somit hinsichtlich der technisch möglichen Erfassung und Änderung von Daten die Arbeitsmarktsprengelverordnung wider. Andere Geschäftsstellen können nur Abfragen für nicht im Zuständigkeitssprengel Wohnende durchführen, sofern sie die entsprechende Rolle (nach Funktion, Aufgabengebiet) innehaben. Ombudsstellen und übergeordnete Organisationseinheiten des AMS benötigen personenbezogene Abfragen zwingend zur raschen Behandlung und Aufarbeitung von Beschwerden aller Art (z. B. Amtshaftung, Volksanwaltschaft, Dienstaufsichtsbeschwerden).

Zu a): Systematische und umfassende Bewertungen persönlicher Umstände Arbeitsuchender samt Entscheidungen auf Basis automatisierter Verfahren finden im Rahmen der Betreuung durch das AMS nicht statt. Es werden zwar offene Stellen automationsunterstützt mit dem Anforderungsprofil Arbeitsuchender abgeglichen, doch geht diesem Abgleich stets eine persönliche Absprache bzw. Vereinbarung mit der betroffenen Person voraus, bei der Kenntnisse und Fähigkeiten wie auch Wünsche der arbeitsuchenden Person in das Suchprofil aufgenommen werden. Es wird darüber ein Betreuungsplan mit der arbeitsuchenden Person angelegt. Die persönliche Vorsprache der Person ist zudem gesetzlich zwingend vorgeschrieben (§ 46 AlVG). Weiters sind Kontrollmeldungen (§ 49 AlVG) gesetzlich vorgesehen. Bloß auf EDV basierende Entscheidungen (lit. a) finden somit nicht statt.

Zu b): Die Verarbeitung **besonderer Kategorien von personenbezogenen Daten** (hier Gesundheitsdaten betreffend die Arbeitsfähigkeit bzw. bestehende gesundheitliche Einschränkungen hinsichtlich der Vermittelbarkeit auf Arbeitsplätze; Art. 9 DSGVO) findet nur in einem geringen Ausmaß statt das (noch) nicht zu einer Folgenabschätzung verpflichtet. Es werden als Gesundheitsdaten nur Daten über Einschränkungen der Arbeitsfähigkeit oder beruflichen Verwendungsmöglichkeit verarbeitet, soweit sie erforderlich sind, um zumutbare Arbeitsvermittlungen durchführen zu können. Das AMS ist von sich aus verpflichtet, die Frage der Arbeitsfähigkeit zu klären, wenn auf objektiven Umständen beruhende Zweifel bestehen (§ 8 AlVG; zB VwGH v. 15.5.2013, 2011/08/0356), da die Erfüllung dieses Kriteriums eine zwingende Voraussetzung für den Leistungserhalt darstellt. Derartige Untersuchungen bzw. Gutachten über die Arbeitsfähigkeit oder verbleibende berufliche Einsatzbereiche bei bestehenden gesundheitlichen Einschränkungen arbeitsfähiger Personen werden regelmäßig im Wege des Kompetenzzentrums Begutachtung der Pensionsversicherungsanstalt erbracht. Das AMS erhält die bescheidmäßigen Feststellungen des Pensionsversicherungsträgers wie auch das berufskundliche Gutachten (Leistungskalkül), wenn Maßnahmen der beruflichen Rehabilitation festgestellt werden.

Bloße „Krankmeldungen“ von arbeitslosen Personen, die zu einer Änderung der Leistungszuständigkeit zwischen AMS und KV-Trägern führen, sind als Leistungsvoraussetzungen zu erfassen, geben aber keine Auskunft über die Art der Erkrankung (Diagnose).

Eine Verarbeitung von **personenbezogenen Daten über strafrechtliche Verurteilungen** (Art. 10 DSGVO) findet nur in wenigen Einzelfällen statt, in denen das AMS Kenntnis über den Tatbestand einer strafrechtlichen Verurteilung erlangt. Kenntnis erlangt das AMS in jenen Fällen, in denen eine Person die

Anwartschaft für Leistungen aufgrund ihrer Beschäftigung während der Haft erworben hat (§ 66a AlVG) oder eine zuerkannte Leistung aufgrund der Verbüßung einer Freiheitsstrafe einzustellen ist (§ 12 Abs. 3 lit. e AlVG). Diese Datenart muss im konkreten Einfall zwar im Akt vermerkt werden, wird darüber hinaus aber nicht verwendet. Die Datenverarbeitung unterstützt auch keine Abfrage oder Aufsummierung über diese Datenart, sodass Auswertungen über Fragen wie zB wie viele Personen ihre Anwartschaft durch Arbeitspflicht während der Verbüßung einer Freiheitsstrafe erworben haben, nicht möglich sind. Dies wurde auch in parlamentarischen Anfragen klargestellt.

Zu c): Eine systematische Überwachung der öffentlichen Bereiche der regionalen Geschäftsstellen findet nicht statt.

Notwendigkeit und Angemessenheiten:

Die vom AMS verarbeiteten Daten betreffen zwangsläufig viele Lebensbereiche der Arbeitsuchenden, da schulische und berufliche Ausbildungen sowie das gesamte Erwerbsleben, sofern es auch mit Zeiten der Arbeitslosigkeit einhergeht, eng mit dem Lauf des Lebens verknüpft sind. Der Gesetzgeber schränkt die Datenverarbeitung sowie auch deren Übermittlung an Dritte daher auf deren Erforderlichkeit hin ein. Der Gesetzgeber ermächtigt die Datenverarbeitung nur soweit, „als diese zur Erfüllung der gesetzlichen Aufgaben eine wesentliche Voraussetzung“ bildet (vgl. zB § 25 Abs. 1 erster Satz AMSG). Dies schließt die Verarbeitung überschießender Daten (auch) nach dem Materiengesetz grundsätzlich aus. Die gesetzliche Ermächtigung zur Datenverarbeitung entspricht damit den in der DSGVO enthaltenen Grundsätzen des Art. 5 Abs. 1 lit. a bis c DSGVO.

Den von der Datenverarbeitung des AMS betroffenen Personen stehen die im Datenschutzgesetz enthaltenen Rechte (§§ 26 bis 28 DSG 2000 idF des Bundesgesetzes BGBl. I Nr. 132/2015) bzw. ab 25. Mai 2018 in Art. 15 bis 21 DSGVO normierten Rechte weiterhin zu. Das AMS hat ein eigenes EDV-Tool entwickelt, das Mitarbeiter/innen die rasche Beantwortung von Auskünften über die verarbeiteten Datenarten ermöglicht und das weiterhin verwendet werden wird.

Risiken und Datensicherheitsmaßnahmen:

Fraglich ist, ob durch die bestehenden Datenverarbeitungen des AMS für die Arbeitsuchenden ein hohes Risiko hinsichtlich einer Verletzung des Schutzes ihrer personenbezogenen Daten vorhanden ist. Auswirkungen einer solchen Verletzung könnten dann den Verlust der Kontrolle über die verarbeiteten Daten, Identitätsdiebstahl oder –betrug, finanzielle Verluste, Diskriminierungen, Rufschädigung und Verlust der Vertraulichkeit durch Bekanntwerden von (Teilen der) Daten gegenüber unbefugten Dritten, eine unbefugte Aufhebung von Pseudonymisierungen oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffenen Personen nach sich ziehen. Im Hinblick auf die hier verarbeiteten Datenarten könnten insbesondere Leistungsdaten von Arbeitslosen wie auch deren persönliche Lebensumstände unbefugten Dritten bekannt werden oder bei einem „Hacker-Angriff“ zerstört oder unbrauchbar werden. Abs. 10 ergänzt nunmehr auch nach dem Materiengesetz zu treffende Datensicherheitsmaßnahmen, wie diese auch im DSG und der DSGVO (Art. 24, 25 und 32) enthalten sind.

So ist die Befugnis bei der Datenverwendung zwischen den Organisationseinheiten und den Mitarbeiterinnen zwingend konkret festgelegt und die Verwendung an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter/innen gebunden. Die Mitarbeiter/innen werden über ihre Pflichten nach dem Datenschutzgesetz (§ 6 DSG idF des Bundesgesetzes BGBl. I Nr. 120/2017) und den innerorganisatorischen Datenschutzvorschriften belehrt und ihr Zugriff auf konkrete Daten ist entsprechend dem Stand der Technik nach Rollen und Aufgaben der Mitarbeiter/innen des AMS entsprechend getrennt gestaltet, sodass Eingaben oder Änderungen personenbezogener Daten nur jenen Bediensteten möglich sind, die für diese Personen zuständig und verantwortlich sind. Es wird außerdem jede Datenabfrage (-änderung) protokolliert, wobei zu jeder Abfrage der Benutzercode der abfragenden Mitarbeiterin (des abfragenden Mitarbeiters), das Kalenderdatum und das Ergebnis der Abfrage (aktueller Stand zum Abfragezeitpunkt) gespeichert wird. Geheimhaltungspflichten sind neben § 27 AMSG umfassend in § 6 DSG idF des Bundesgesetzes BGBl. I Nr. 120/2017 geregelt, sodass ein weiterer Absatz in § 25 AMSG nicht erforderlich ist.

Die vom AMS gesetzten Sicherheitsmaßnahmen entsprechen dem geforderten Standard (Abs. 10), womit im Ergebnis durch die Datenverarbeitungen des AMS kein hohes Risiko für den Schutz personenbezogener Daten der Arbeitsuchenden besteht.

Zu Art. 42 Z 2 (§ 78 Abs. 35 AMSG):

Die Anpassungen im AMSG sollen mit 25. Mai 2018 in Kraft treten.

Zu Art. 43 (Änderung des IEF-Service-GmbH-Gesetzes):

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 11 B-VG.

Zu Art. 43 Z 1 (§ 19 Abs. 1 IEFG):

In § 19 Abs. 1 sollen Bestimmungen zur Datenverarbeitung der IEF-Service-GmbH, soweit diese gesetzlich übertragene Aufgaben vollzieht, zusammengefasst und insbesondere die verarbeiteten Datenarten ausführlicher als bisher in § 5 Abs. 5 IESG aufgelistet werden.

Die IEF-Service-GmbH betreibt für die Erfüllung der ihr gesetzlich übertragenen Aufgaben (Entscheidungen über Ansprüche auf Insolvenzentgelt und Betreibung der auf sie übergegangenen Forderungen) eine zentrale Datenverarbeitung, die (bis Ablauf des 24. Mai 2018) beim DVR unter 1075900/001 „Erstellung von Bescheiden und Geltendmachung von übergegangenen Forderungen nach dem Insolvenz-Entgeltsicherungsgesetz (IESG)“ registriert ist. Diese Datenverarbeitung dient der IEF-Service GmbH bei der Bearbeitung von Geschäftsfällen insolventer Unternehmen und der davon betroffenen Antragsteller und Antragstellerinnen. Diese werden nachvollziehbar und durchgängig in einer Web-Anwendung inklusive eines Dokumentmanagements abgebildet. Unterstützt durch das Workflow-Management gelangt der Geschäftsfall – nachvollziehbar – an den richtigen Empfänger. Dabei stehen durchgängig alle Stadien von der Erfassung des Eingangs bis zum Abschluss und der Archivierung eines Geschäftsfalls zur Verfügung.

Der Begriff der Anspruchsberechtigten in Abs. 1 ist aus teleologischen Gründen weit zu interpretieren. Er umfasst sämtliche Personen, die einen Antrag oder eine Anfrage betreffend einen Anspruch auf Insolvenzentgelt stellen. Er umfasst auch Anfragen für Anspruchsberechtigte, die von berechtigten Dritten gestellt werden, die von der IEF-Service GmbH wissen wollen, ob eine konkrete Person einen Anspruch auf Insolvenzentgelt haben wird, auch wenn zum Zeitpunkt der Anfrage noch kein formeller Antrag erfolgt ist. Unter berechtigten Dritten sind der Insolvenzverwalter, der Insolvenzschutzverband für ArbeitnehmerInnen (ISA) und auch Exekutionsgläubiger von Anspruchsberechtigten zu verstehen, die sich in der Praxis teilweise schon vor formellen Anträgen erkundigen, ob bzw. inwieweit überhaupt eine Anspruchsberechtigung vorliegt oder vorliegen könnte.

Unter „Schuldner“ sind jene Personen zu verstehen, denen gegenüber die IEF-Service-GmbH Forderungen hat. Darunter fallen – neben dem Schuldner im Insolvenzverfahren – Personen, deren (ehemalige) Ansprüche zu widerrufen und zurück zu fordern sind, weil sie zB durch unwahre Angaben oder Verschweigung maßgebender Tatsachen herbeigeführt wurden oder weil der Anspruch wegen einer späteren Verurteilung iS § 1 Abs. 3 Z 1a IESG wegfällt. Weiters sind darunter auch jene Arbeitgeber sowie deren Organe zu subsumieren, die im Zusammenhang mit der Insolvenz iS des § 11 Abs. 3 letzter Satz IESG strafrechtlich verurteilt wurden, sowie auch dritte Personen, die für das insolvente Unternehmen gesetzlich haften, Haftungen als Bürgen eingegangen sind oder vom IEF als Insolvenzgläubiger für Schadenersatz in Anspruch genommen werden können.

Unter Beschäftigungsdaten sind Beschäftigungszeiträume der (möglicherweise) Anspruchsberechtigten und Schuldner, wie Beginn und Ende von Beschäftigungen, deren Dienstgeber, Beitragsgrundlagen und Art der Beschäftigung (Qualifikationen) zu verstehen. Unter Lohnverrechnungsdaten sind jene Datenarten zu subsumieren, die in der Standardanwendung Personalverwaltung für privatrechtliche Dienstverhältnisse, SA0002 der Anlage 1 der Standard- und Musterverordnung 2004, BGBl. II Nr. 312/2004, in der Fassung der Verordnung BGBl. II Nr. 278/2015, enthalten sind. Da Insolvenzentgelt „netto“ gebührt (§ 3 Abs. 1 IESG) und ausbezahlt wird, d.h. unter Abzug all jener Beträge, die üblicherweise der Arbeitgeber vom Bruttoentgelt abzieht, hat die IEF-Service GmbH – vergleichbar einem Arbeitgeber – das jeweilige Nettoentgelt zu ermitteln und folglich auszuzahlen. In diesem Sinne muss die IEF-Service GmbH für die Berechnung dieses „Nettobetrages“ – je nach Einzelfall des Anspruchsberechtigten bzw. Antragstellers auch jene Daten verarbeiten, die ein Arbeitgeber für die Berechnung des Lohnes verarbeiten muss. Insbesondere sind nicht nur Sozialversicherungsbeiträge abzuziehen, sondern – soweit eine Mitgliedschaft gegeben ist – etwa auch Gewerkschaftsbeiträge oder bei Ende des Dienstverhältnisses vorhandene Lohnvorschüsse zu berücksichtigen. Im Falle einer Lohnpfändung eines Anspruchsberechtigten sind auch diese Daten zu verarbeiten. Das weite Spektrum an Datenarten der Lohnverrechnung kommt freilich nur soweit zur Verarbeitung, als dies für die Berechnung des Insolvenz-Entgeltes auch erforderlich ist. Der Verhältnismäßigkeitsgrundsatz des § 1 Abs. 2 DSG bleibt somit gewahrt.

Unter „Daten zu Eigentumsverhältnissen an Immobilien“ sind Auszüge aus dem Grundbuch zu verstehen, die zum Zwecke der Betreibung der auf den IEF übergegangenen Forderungen abgefragt werden.

Zu Art. 43 Z 1 (§ 19 Abs. 2 IEFG):

Die Aufbewahrungsfrist hinsichtlich der Daten insolventer Betriebe und von deren Beschäftigten, die Anträge auf Insolvenzentgelt gestellt haben, folgt dem § 212 Abs. 1 UGB. Einem Insolvenzverfahren stehen die in § 1 Abs. 1 IESG genannten Verfahren (wie zB Anordnung der Geschäftsaufsicht, Nichteröffnung oder Ablehnung eines IO-Verfahrens mangels Kostendeckung oder Vermögenslosigkeit) gleich. Ein längerer Bedarf an den Daten kann sich v.a. bei Personen ergeben, deren Anspruch von der IEF-Service GmbH gemäß § 9 Abs. 1 IESG zurückgefordert wird, wenn das Strafverfahren längere Zeit in Anspruch nimmt sowie bei Zugriff auf zukünftiges Vermögen gemäß § 11 Abs. 3 IESG im Betreibungsfall. Insbesondere für diese Fälle wird durch die vorgesehene Fristverlängerung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vorgesorgt.

Zu Art 43 Z 1 (§ 19 Abs. 3 bis 5 IEFG):

Abs. 3 und 4 geben den von der IEF-Service GmbH zu beachtenden Standard an technischen und organisatorischen Datensicherheitsmaßnahmen wieder. Dabei handelt es sich um einen Standard, wie er auch nach den Bestimmungen des Datenschutzgesetzes und der DSGVO (Artikel 24f) gefordert ist.

Gemäß Art. 35 Abs. 1 der DSGVO haben Verantwortliche eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Datenverarbeitung **neue Technologien** verwendet oder **Art, Umfang, Umstände und Zweck der Verarbeitung** voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Beispielhaft sind die Verarbeitungen aufgezählt, bei denen

a) sich eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen einschließlich Profiling samt darauf folgender Entscheidungen auf eine automatisierte Verarbeitung gründet,
b) eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (wie Gesundheitsdaten oder Daten über strafrechtliche Verurteilungen) oder
c) eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

Von den genannten literae ist für die Datenverarbeitung der IEF-Service GmbH lit. b näher zu erläutern, da Abs. 1 Z 3 und 5 Datenarten gemäß Art. 10 DSGVO und Z 2 allenfalls Datenarten gemäß Artikel 9 DSGVO enthalten.

Zweck und Notwendigkeit der Datenverarbeitung ergeben sich klar aus den gesetzlichen Bestimmungen, die die Sicherung des Entgelts von Beschäftigten bei Insolvenz des Arbeitgebers gewährleisten. Das IESG dient der Umsetzung der Richtlinie 2008/94/EG vom 22. Oktober 2008 über den Schutz der Arbeitnehmer bei Zahlungsunfähigkeit des Arbeitgebers in nationales Recht.

Die in Abs. 1 angeführten Datenarten sind für die Erfüllung der gesetzlichen Aufgaben der IEF-Service GmbH erforderlich. So sind – wie bereits erwähnt – die in Abs. 1 Z 2 angeführten Datenarten (Lohnverrechnungsdaten) für die Nettoberechnung des Insolvenz-Entgeltes erforderlich. Dies schließt die vom Arbeitnehmer gegebenenfalls dem Arbeitgeber übertragenen Abzüge von Gewerkschaftsbeiträgen vom Bruttolohn mit ein. Die Verarbeitung dieser Daten in jenen Fällen, in denen der Arbeitgeber zu diesen Abzügen ermächtigt wurde, greift nicht stärker in das Recht auf Schutz personenbezogener Daten ein, als dies bisher durch den jeweiligen Arbeitgeber im Rahmen der Standardanwendung SA002 (Personalverwaltung für privatrechtliche Dienstverhältnisse) möglich und zulässig ist. Diese Daten werden nur je Einzelfall, wo diese Ermächtigung des Arbeitgebers besteht, in den jeweiligen Personenunterlagen verarbeitet, ohne dass eine Aufsummierung über alle Antragsteller möglich ist. Insoweit besteht auch keine Gefährdung berechtigter Interessen der Antragsteller.

Um nicht jene Personen, die im Zusammenhang mit einer Insolvenz strafrechtlich verurteilt wurden, durch die ausbezahlten Leistungen (noch) zu belohnen, sieht das IESG in diesen Fällen eine Rückforderung der auf den Insolvenz-Entgelt-Fonds übergegangenen Forderungen vor (§ 9 Abs. 1 in Verbindung mit § 1 Abs. 3 Z 1a IESG). Die Verarbeitung der entsprechenden Daten ist daher unabdingbar, um die Forderungen betreiben zu können.

Lassen die bei der Antragstellung auf Insolvenz-Entgelt erhobenen Daten einen Verdacht auf strafbare Handlungen aufkommen, so erfolgt eine Meldung an die anderen Kooperationsstellen gemäß § 4 Abs. 2 des Sozialbetrugsbekämpfungsgesetzes. Die IEF-Service GmbH speichert diese Daten (Antrag/Insolvenz/Betreibungsfall) für den eigenen gesetzlichen Zweck der Entgeltsicherung für sieben Jahre (Abs. 2). Die Löschung von Daten über ein laufendes Strafverfahren gegen einen Antragsteller (zu § 9 Abs. 1 IESG) bzw. zu einem Betreibungsfall (zu § 11 Abs. 3 IESG) wird hingegen bis zum Ablauf dieses Verfahrens ausgesetzt. In Folge wird bei einer Verurteilung ein Rückforderungsbescheid erstellt bzw. der Zugriff auf das Vermögen des Verurteilten gemäß § 11 Abs. 3 IESG versucht. Bei Abschluss des Verfahrens ohne Verurteilung werden die Daten umgehend bzw. nach Ablauf der regulären Löschfrist gelöscht.

Datenarten gemäß Art. 10 DSGVO werden nur in einem geringen Umfang verarbeitet, sodass nicht von einem hohen Risiko für Rechte und Freiheiten der betroffenen Personen ausgegangen werden kann. Dies aus folgenden Gründen:

Der Anteil der Arbeitgeber unter (anfänglichem) Verdacht auf Sozialbetrug an allen im gesamten Jahr 2016 eröffneten Insolvenzen (= Arbeitgeber) betrug lediglich 3,6%. Dies entspricht in etwa auch dem Durchschnitt der Jahre 2008 bis 2016.

Der Anteil der Betreibungsfälle mit den einschlägigen Straftatbeständen (des § 11 Abs. 3) ist auch aufgrund der langen Betreibungszeiten nicht direkt erhebbar. Feststellbar ist aber, wie viele Informationsschreiben (Informationen über Strafverfahren) in einem Jahr eingegangen sind und wie viele entsprechende Klagen seitens des IEF eingebracht wurden. Sieht man sich im Vergleich dazu an, wie viele Betreibungsfälle insgesamt in einem Jahr zugegangen sind, lässt sich feststellen, dass der Anteil offensichtlich sehr gering ist:

Jahr	BF/Schreiben	Klagen bei 11 (3)	zugeg. BF gesamt
2014	5	3	2.552
2015	27	4	2.433
2016	27	0	2.440
2017	20	0	1.474

Der Anteil der Rückforderungen (insbesondere derjenigen, die auf strafrechtliche Verurteilungen zurückzuführen sind) kann derzeit auch aufgrund der langen gesetzlichen Frist für Rückforderungen – fünf Jahre ab Kenntnis des Rückforderungsgrundes – nicht direkt erhoben werden. Festgestellt werden kann aber, dass der Anteil an rückgeforderten Leistungen an sich äußerst gering ist. Beispielsweise ergingen im Jahr 2016 40 Rückforderungen gegenüber insgesamt 39.454 erlassenen Bescheiden, was im Verhältnis auch dem Schnitt der Jahre 2011 bis 2016 entspricht.

Zu Art 43 Z 1 (§ 19 Abs. 6 IEFG):

Die IEF-Service GmbH ist in der Erfüllung der ihr gesetzlich übertragenen Aufgaben Verantwortliche des öffentlichen Bereiches gemäß § 26 Abs. 1 Z 2 DSG und öffentliche Stelle im Sinne des § 30 Abs. 5 DSG. Die gesetzlich übertragenen Aufgaben umfassen neben der Prüfung, Berechnung und Auszahlung des Insolvenzentgeltes auch die Betreibung der auf den IEF nach § 11 übergegangenen Forderungen sowie deren Geltendmachung gegenüber dritten Personen (Bürgen, Mithaftende, Insolvenzverwalter aufgrund von Schadenersatzansprüchen, etc.) sowie die Verfolgung von Regressansprüchen nach § 11 Abs. 3 IESG.

Zur Vermeidung von Auslegungsproblemen und Rechtsstreitigkeiten soll mangels Legaldefinition im DSG (anders als etwa in § 4 IWG) – klargestellt werden, dass die IEF-Service GmbH eine öffentliche Stelle im Sinne der Datenschutz-Grundverordnung und des Datenschutzgesetzes ist.

Zu Art. 44 (Änderung des Insolvenz-Entgeltsicherungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 44 Z 1 und 2 (§ 5 Abs. 5 und § 14 Abs. 4 IESG):

Durch die Einfügung der Bestimmungen zur Datenverarbeitung der IEF-Service GmbH in § 19 IEFG kann § 5 Abs. 5 IESG entfallen und der Wortlaut des § 14 Abs. 4 IESG vereinfacht werden. § 14 Abs. 4 ermöglicht die für die Erfüllung der gesetzlich übertragenen Aufgaben jeweils erforderlichen Abfragen von Beschäftigungs- und Versicherungszeiten aus der Versicherungsdatenbank des Hauptverbandes. Für die erforderliche Unterstützung der Träger der Sozialversicherung (§ 14 Abs. 1) ist daher – soweit dies ausreichend ist – auch in erster Linie die dafür geschaffene Abfragemöglichkeit der beim Hauptverband gespeicherten Beschäftigungs- und Versicherungszeiten zu nutzen. Nur soweit dies nicht ausreicht, sind zusätzliche Anfragen auf Amtshilfe zu stellen.

§ 14 Abs. 4 soll um die Möglichkeit der Abfrage von Beschäftigten je Dienstgeber(konto) ergänzt werden, weil diese Abfragemöglichkeit der IEF-Service GmbH die Prüfung, ob ein Betriebsübergang nach § 3 AVRAG vorliegt, wesentlich erleichtert. Eine derartige Prüfung ist erforderlich und

zweckmäßig, da im Falle eines Betriebsüberganges in der Regel der Erwerber für das aushaftende Entgelt haftet und somit kein Anspruch auf Insolvenz-Entgelt gegeben ist. Die Abfrage soll die IEF-Service GmbH zudem bei der Aufdeckung von Sozialbetrugsfällen unterstützen.

Zu Art. 44 Z 3 (§ 36 IESG):

Die Neuregelung soll mit 25. Mai 2018 in Kraft treten.

Zu Art. 45 (Änderung des Bauarbeiter-Urlaubs- und Abfertigungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 11 B-VG.

Zu Art. 45 Z 1 (§ 31a Abs. 2 BUAG):

Die DSGVO macht die Zulässigkeit einer Datenverarbeitung vom Vorliegen eines Erlaubnistatbestandes abhängig. Diese sind in den Art. 6 und 9 DSGVO konkretisiert. Bisher war die Weitergabe von Informationen durch die Urlaubs- und Abfertigungskasse entsprechend dem Datenschutzgesetz 2000 als Ermächtigung formuliert. Da es sich dabei um eine zur Erfüllung ihrer Aufgaben notwendige Datenverarbeitung handelt, soll diese Bestimmung künftig als gesetzliche Verpflichtung formuliert werden. Damit fällt sie unter den datenschutzrechtlichen Erlaubnistatbestand des Art. 6 Abs. 1 lit c) DSGVO.

Zu Art. 45 Z 2 und 3 (§ 31a Abs. 4 und 5 BUAG):

§ 31a beinhaltete bisher entsprechend dem DSG 2000 Datenschutzbestimmungen im Zusammenhang mit dem Betreiben der Baustellendatenbank durch die Urlaubs- und Abfertigungskasse. Künftig gelten für die Urlaubs- und Abfertigungskasse als Verantwortliche im Sinne der DSGVO die in dieser VO und im Datenschutz-Anpassungsgesetz 2018, BGBl I Nr. 120/2017 vorgesehenen Regelungen (vgl. Art. 24 iVm Art. 32 DSGVO). Die Sonderregelungen der Abs. 4 und 5 sind daher weitgehend zu streichen. Lediglich die Verpflichtung der Urlaubs- und Abfertigungskasse, Daten nach spätestens sieben Jahren zu löschen (siehe Abs. 4), soll aufrecht bleiben, um die rechtmäßige Verarbeitung der personenbezogenen Daten iSd Art. 6 Abs. 1 lit. c) iVm Art. 6 Abs. 2 DSGVO sicherzustellen.

Zu Art. 45 Z 4 (§ 33g Abs. 1 und 2 BUAG):

Diese Zitatanpassungen dienen der Bereinigung eines Redaktionsversehens.

Zu Art. 46 (Änderung des Lohn- und Sozialdumping-Bekämpfungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 6 und 11 B-VG.

Zu Art. 46 Z 1 und 2 (§ 11 Abs. 2 und 3 LSD-BG):

In diesen Bestimmungen erfolgen jeweils erforderliche Begriffsanpassungen.

Zu Art. 46 Z 3 (§ 11 Abs. 4 LSD-BG):

Derzeit sieht § 11 Abs. 4 erster Satz LSD-BG vor, dass auf die sich aus dem LSD-BG ergebenden Tätigkeiten der Abgabenbehörden und des Kompetenzzentrums LSDB § 14 DSG 2000 anzuwenden ist, welcher Datensicherheitsmaßnahmen betrifft. Künftig werden sich entsprechende Verpflichtungen aus der DSGVO ergeben. Um keinen allgemeinen Verweis – ohne Mehrwert – auf die DSGVO vorzusehen, soll § 11 Abs. 4 erster Satz LSD-BG nicht angepasst werden, sondern ersatzlos entfallen.

Zu Art. 47 (Änderung des Sozialbetrugsbekämpfungsgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 47 Z 1 (Überschrift zu § 5):

Es soll dem Umstand Rechnung getragen werden, dass die Datenbank nach § 5 SBBG nicht mehr als Informationsverbundsystem geführt wird.

Zu Art. 47 Z 2 (§ 5 Abs. 3 und 4):

Die neuen datenschutzrechtlichen Bestimmungen sehen kein Informationsverbundsystem vor. Dies soll im § 5 Abs. 3 SBBG entsprechend berücksichtigt werden. Neue Regelungen zur Aufgabenverteilung

sollen in einem neuen Abs. 6 vorgesehen werden (dazu unten). Weiters sollen aufgrund der neuen datenschutzrechtlichen Terminologie Begriffsanpassungen vorgenommen werden.

Im Abs. 4 sollen ebenfalls erforderliche datenschutzrechtliche Begriffsanpassungen vorgenommen werden. Weiters soll bei Bezugnahmen auf gewisse Absätze dem Umstand Rechnung getragen werden, dass sich der Regelungsinhalt des bisherigen Abs. 6 künftig in einem neuen Absatz 7 finden soll.

Zu Art. 47 Z 3 (§ 5 Abs. 6):

In einem neuen Abs. 6 sollen Regelungen vorgesehen werden, die aufgrund des Umstands des Entfalls des Informationsverbundsystems für die Rechte der betroffenen Personen erforderlich werden.

Zu Art. 47 Z 4 (§ 8 Abs. 10):

Veröffentlichungen, die sich auf natürliche Personen beziehen, sollen nach Ablauf von fünf Jahren nach der Veröffentlichung zu löschen sein.

Zu Art. 48 (Änderung des Ausbildungspflichtgesetzes)

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 48 Z 1 bis 3 (§ 13 und 15):

Es werden lediglich terminologische Anpassungen an die DSGVO vorgenommen.

Zu Art. 48 Z 4 (§ 21):

Die Regelung soll mit 25. Mai 2018 in Kraft treten.

Zu Art. 49 (Änderung des Arbeiterkammergesetzes 1992):

Kompetenzgrundlage:

Die Zuständigkeit des Bundes gründet sich auf Art. 10 Abs. 1 Z 11 B-VG.

Zu Art. 49 Z 1 (§ 17a Abs. 4 AKG), 8 und 9 (§ 45 Abs. 1 und 2 erster Satz AKG) sowie 11 bis 13 (§ 92AKG)

Die Datenschutz-Grundverordnung macht die Zulässigkeit einer Datenverarbeitung vom Vorliegen eines Erlaubnistatbestandes abhängig. Diese sind in den Art. 6 und 9 DSGVO konkretisiert. Bisher war die Datenverarbeitung durch die Arbeiterkammern entsprechend dem Datenschutzgesetz 2000 als Ermächtigungen zur Datenverarbeitung formuliert. Da es sich bei der Datenverarbeitung nach § 45 als auch nach § 92 um eine zur Erfüllung ihrer Aufgaben notwendige Datenverarbeitungen handelt, sollen diese Bestimmungen künftig als gesetzliche Verpflichtungen formuliert werden. Damit fallen sie unter den datenschutzrechtlichen Erlaubnistatbestand des Art. 6 Abs. 1 lit. c) DSGVO. § 17a Abs. 4 stellt die gesetzliche Verarbeitungsgrundlage (Verpflichtung iSd Art. 6 Abs. 1 lit. c DSGVO) durch die Arbeiterkammer dar.

Zu Art. 49 Z 1, 2, 4, 5, 6, 7, 9, 10 und 13 (§ 17a Abs. 4 und 5, § 33 Abs. 3 und 4, § 34 Abs. 2 und 4, § 45 Abs. 2 und 3 AKG):

Hier erfolgen terminologische Anpassungen an die DSGVO (wie beispielsweise das Ersetzen des Begriffes „Daten“ durch „personenbezogene Daten“ oder das Ersetzen des Begriffes „verwenden“ durch „verarbeiten“).

Zu Art. 49 Z 3 (§ 18 Abs. 5 AKG)

Hier handelt es sich um die Beseitigung eines Redaktionsversehens.

Zum 4. Hauptstück (Bildung)

Allgemeines:

Umsetzung der Datenschutz-Grundverordnung

Trotz unmittelbarer Geltung in den Mitgliedstaaten bedarf die Datenschutz-Grundverordnung in zahlreichen Bereichen der Durchführung in innerstaatliches Recht. *So enthält sie – unbeschadet des Transformationsverbots und der damit verbundenen mangelnden Rechtssetzungskompetenz der Mitgliedstaaten – zahlreiche Regelungsspielräume bzw. „Öffnungsklauseln“, die den nationalen Gesetzgeber verpflichten oder berechtigen, im Rahmen der Vorgaben des Art. 6 Abs. 2 und 3 iVm Art. 6 Abs. 1 lit. c und e DSGVO bestimmte Angelegenheiten näher zu regeln. Soweit in der Verordnung*

Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, ist es zudem zulässig, dass die Mitgliedstaaten – zur Wahrung der Kohärenz und um nationale Vorschriften verständlicher zu machen – Teile dieser Verordnung in ihr nationales Recht aufnehmen (vgl. ErwGr 8 zur DSGVO).

Auch gemäß § 69 Abs. 8 des Datenschutzgesetzes sind – im Rahmen der Vorgaben durch die DSGVO – in Bundes- und Landesgesetzes besondere Bestimmungen über die Verarbeitung von personenbezogenen Daten, die vom DSG abweichen, zulässig.

Materienspezifische Datenschutzregelungen können im Rahmen der Vorgaben der DSGVO auch weiterhin auf die Kompetenztatbestände der jeweiligen Materie gestützt werden (Annexmaterie).

Im Bereich des Schul- und Hochschulwesens bestehen spezifische datenschutzrechtlich relevante Regelungen vor allem im Bildungsdokumentationsgesetz, BGBl. I Nr. 12/2002, aber auch im Schulunterrichtsgesetz, BGBl. Nr. 472/1986, im Schulunterrichtsgesetz für Berufstätige, Kollegs und Vorbereitungslehrgänge, BGBl. I Nr. 33/1997, im Schulpflichtgesetz 1985, BGBl. Nr. 76/1985, im BIFIE-Gesetz 2008, BGBl. I Nr. 25/2008, im Hochschulgesetz 2005, BGBl. I Nr. 30/2006, sowie im Schülerbeihilfengesetz 1983. Diese Regelungen sind auf ihre Vereinbarkeit mit der DSGVO zu überprüfen und gegebenenfalls anzupassen. Die erforderlichen Adaptierungen erfolgen im Rahmen des als Entwurf vorliegenden Gesetzespaketes.

Da das Datenschutzregime der DSGVO neue Begrifflichkeiten vorsieht, sind in den materienspezifischen Bestimmungen zahlreiche terminologische Anpassungen erforderlich. Diesen folgen vor allem im Bildungsdokumentationsgesetz zum Teil nicht unerhebliche inhaltliche Änderungen, die den Datenverbund der Universitäten und Pädagogischen Hochschulen, der nach der bis 25. Mai 2018 geltenden Rechtslage als Informationsverbundsystem im Sinne des § 4 Z 13 iVm § 50 DSG 2000 ausgestaltet ist, betreffen. Da der DSGVO das Informationsverbundsystem im Sinne des (durch die Novelle BGBl. I Nr. 120/2017 außer Kraft tretenden) § 4 Z 13 DSG 2000 fremd ist, sind hier Anpassungen vorzunehmen. Ein Informationsverbundsystem lag nach bisheriger Rechtslage vor, wenn mehrere Auftraggeber die von ihnen verarbeiteten Daten in ein gemeinsames System einspeisten und jeder Auftraggeber Zugriff auf sämtliche in diesem System verarbeiteten Daten hatte. Die Weiterführung des bewährten Datenverbundes der Universitäten und Pädagogischen Hochschulen, erweitert um die Fachhochschulen und Fachhochschul-Studiengänge sowie die Privatuniversitäten, soll nunmehr über die in Art. 26 DSGVO geschaffene „gemeinsame Verantwortlichkeit“ der beteiligten Bildungseinrichtungen ermöglicht werden. Neben den Regelungen des Datenverbundes gemäß § 7a des Bildungsdokumentationsgesetzes soll mit der Verankerung des „Austrian Higher Education Systems Network“ (§ 7b des Bildungsdokumentationsgesetzes in der Fassung des vorliegenden Entwurfs) für den universitären und hochschulischen Bereich ausschließlich zum Zweck der Gewährleistung der ordentlichen Verwaltung und Durchführung von gemeinsamen Studienprogrammen und gemeinsam eingerichteten Studien eine eigene gesetzliche Grundlage geschaffen werden. Im Gegensatz zum Datenverbund soll beim AHESN keine eigene Datenbank befüllt werden, sondern eine Verarbeitung bzw. Übermittlung der für die Verwaltung und Durchführung eines gemeinsamen Studienprogramms oder eines gemeinsam eingerichteten Studiums erforderlichen Daten „nur“ zwischen den an einem gemeinsamen Studienprogramm oder an einem gemeinsam eingerichteten Studium beteiligten Bildungseinrichtungen erfolgen („Peer-to-Peer“-Architektur“).

Die notwendigen Änderungen des Bildungsdokumentationsgesetzes werden weiters zum Anlass genommen, auch im Bereich der Schulen einen dem universitären und hochschulischen Bereich nachgebildeten Datenverbund der Schulen (§ 7c sowie Anlage 4 in der vorliegenden Entwurfsfassung) zu implementieren. Dieser soll zur Vollziehung der mit der Aufnahme von Schülerinnen und Schülern in Zusammenhang stehenden Rechtsvorschriften eingerichtet werden, dient dem Zweck der Vollständigkeit und der Richtigkeit der bei einem Schulwechsel in den lokalen Evidenzen zu verarbeitenden Schülerdaten und soll den derzeit nicht unerheblichen Verwaltungsaufwand an den Schulstandorten bei der Aufnahme von Schülerinnen und Schülern verringern.

Zu Art. 50 (Änderung des Bildungsdokumentationsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 13 B-VG, Art. 14 Abs. 1 B-VG und Art. 14a Abs. 2 B-VG.

Zu Art. 50 Z 1, 2 und 3 (Inhaltsverzeichnis zu den §§ 7a, 7b, 7c und 10a sowie zur Anlage 4):

Hier erfolgt eine Anpassung des Inhaltsverzeichnisses betreffend den Datenverbund der Universitäten und Hochschulen (§ 7a), das gesetzlich neu verankerte „Austrian Higher Education Systems Network“ (§ 7b),

den ebenfalls gesetzlich neu verankerten Datenverbund der Schulen (§ 7c sowie die zugehörige Anlage 4) sowie die Änderung der Überschrift des § 10a.

Zu Art. 50 Z 4 (§ 1):

Die bisherige Textierung des § 1 soll, mit Ausnahme folgender notwendiger Anpassungen aufgrund der unmittelbaren Geltung der DSGVO, inhaltlich unverändert als Abs. 1 neu gefasst werden:

In Abs. 1 Z 1 wird hinsichtlich der Verarbeitung personenbezogener Daten auf die unmittelbar anwendbare DSGVO verwiesen.

In Abs. 1 Z 3 soll der Begriff „Verwendung“ im Sinne des § 4 DSG 2000 in der Fassung vor dem Datenschutz-Anpassungsgesetz 2018 durch den Begriff „Verarbeitung“ (Art. 4 Z 2 DSGVO) ersetzt werden.

In einem neuen Abs. 2 soll die Anwendbarkeit des 1. und des 2. Abschnitts des Forschungsorganisationsgesetzes, BGBl. Nr. 341/1981, auch im Anwendungsbereich des Bildungsdokumentationsgesetzes vorgesehen werden, soweit dieses keine abweichenden Bestimmungen enthält. Die zukünftige Anwendbarkeit des wissenschaftlichen Sonderdatenschutzrechts ergibt sich zwar bereits aus § 1 Abs. 1 Z 1 des Forschungsorganisationsgesetzes in der Fassung eines parallel geplanten Datenschutz-Anpassungsgesetzes für den Bereich der Wissenschaft und Forschung, wonach allgemeine Angelegenheiten der Tätigkeiten zu Zwecken gemäß Art. 89 Abs. 1 DSGVO sowie der Verarbeitung von Daten, soweit diese für Zwecke gemäß Art. 89 DSGVO erfolgt, Gegenstand des Forschungsorganisationsgesetzes sind. Allerdings soll aus Gründen der Rechtssicherheit durch den neu eingefügten Abs. 2 klargestellt werden, dass die Spezialbestimmungen des 1. und 2. Abschnitts des Forschungsorganisationsgesetzes jedenfalls auch für die vom Bildungsdokumentationsgesetz umfassten und in Frage kommenden Einrichtungen gelten.

Zu Art. 50 Z 5, 6, 7, 8 und 9 (§ 2 Abs. 1 Z 1 lit. a und c, Z 2 lit. b, e und f; Entfall des § 2 Abs. 1 Z 2 lit. g; § 2 Abs. 1 Z 3):

Hier sollen rein redaktionelle Anpassungen aufgrund geänderter schul- und hochschulrechtlicher Regelungen erfolgen.

Zu Art. 50 Z 10 (§ 2 Abs. 1 Z 6):

Im Bildungsdokumentationsgesetz wird die „Verarbeitung“ unterschiedlicher Kategorien von Daten geregelt. Zum einen handelt es sich dabei um personenbezogene Daten im Sinne des Art. 4 Z 1 DSGVO, worunter „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen, zu verstehen sind. Zum anderen wird auch die Verarbeitung von Informationen geregelt, die nicht oder nicht mehr in den Anwendungsbereich der DSGVO fallen, da sie nur (mehr) in (absolut oder relativ) anonymer bzw. anonymisierter Form vorliegen. Darunter fallen zB Informationen, die sich nie auf eine natürliche Person bezogen haben (vgl. auch § 4 des Bildungsdokumentationsgesetzes) oder Informationen hinsichtlich derer eine natürliche Person nicht identifiziert oder nicht bzw. nicht mehr identifizierbar ist oder bei denen es nach allgemeinem Ermessen unter Berücksichtigung aller Mittel als unwahrscheinlich erachtet wird, dass ein Personenbezug tatsächlich hergestellt wird (ErwGr 26).

Nunmehr soll eine Begriffsbestimmung zum Begriff „Daten“ in § 2 verankert werden, die sämtliche personenbezogene Daten gemäß Art. 4 Z 1 DSGVO und nicht in den Anwendungsbereich der DSGVO fallende Informationen, die aufgrund des Bildungsdokumentationsgesetzes verarbeitet werden, umfasst.

Zu Art. 50 Z 11 (§ 2 Abs. 3):

Der bisher in § 4 Z 4 DSG 2000 definierte Begriff des Auftraggebers ist in sämtlichen Bestimmungen des Bildungsdokumentationsgesetzes durch den Begriff des Verantwortlichen im Sinne des Art. 4 Z 7 DSGVO zu ersetzen. Mit der Novelle BGBl. I Nr. 24/2008 wurden die Leiter bzw. Leiterinnen (wie sie in § 2 Abs. 1 Z 5 definiert sind) der vom Bildungsdokumentationsgesetz umfassten Bildungseinrichtungen als Auftraggeber im Sinne des DSG 2000 definiert. Dies deshalb, da davor bezüglich der Schulen zum Teil Unklarheit darüber bestanden hat, ob deren Leiter oder die Schulbehörde als „Auftraggeber“ für die gesetzlich angeordneten Datenverarbeitungen anzusehen sind.

Die Erläuterungen zur RV 259 BlgNR 23. GP führen dazu aus.

„Schulen sind nach allgemein anerkannter Rechtsauffassung „unselbständige Anstalten“, denen (grundsätzlich) keine Rechtspersönlichkeit zukommt. Dennoch ist der „bescheidähnliche Charakter“ schulischer Entscheidungen rechtlich unbestritten. Dazu kommt, dass Schulen zumeint [sic] ohne Rechtsakt mit Außenwirkung errichtet werden und somit ein Errichtungsakt nicht auf eine konkrete Norm (Gesetz, Verordnung, Bescheid) zurückgeführt werden kann. Tatsächlich entspricht das Handeln der Leiter von Schulen in Vollziehung des Bildungsdokumentationsgesetzes aber dem eines Auftraggebers im

Sinne des DSG 2000. Es erscheint daher zweckmäßig und im Sinne der Rechtsklarheit geboten, die Leiter von Bildungseinrichtungen (wie sie in § 2 Abs. 1 Z 5 definiert sind) ausdrücklich per Gesetz als Auftraggeber im Sinne des § 4 Z 4 DSG 2000 zu definieren. Dies erfolgt der Vollständigkeit und Rechtssicherheit halber in umfassender Form sowohl für die Bildungseinrichtungen des Schulbereichs als auch für jene des Wissenschaftsbereichs. Eine Ausnahme besteht für die Fachhochschulen, hier gelten die Fachhochschul-Erhalter an Stelle der Studiengangsleiter, die für die Zulassung zum Studium zuständig sind, als Auftraggeber, da diese für die Datenverwaltung verantwortlich sind."

Im Sinne dieser Ausführungen soll die datenschutzrechtliche Verantwortlichkeit auch nach den Bestimmungen der DSGVO bei den Leiterinnen und Leitern der Bildungseinrichtungen verbleiben.

Die Zulässigkeit für die gesetzliche Verankerung der Leiterinnen und Leiter der Bildungseinrichtungen als Verantwortliche ergibt sich aus der (fakultativen) Öffnungsklausel des Art. 4 Z 7 2. Halbsatz DSGVO.

Zu Art. 50 Z 12 (§ 2 Abs. 4):

Grundsätzlich soll, wie zu § 2 Abs. 3 bereits ausgeführt, die datenschutzrechtliche Verantwortlichkeit alleine bei der Leiterin oder beim Leiter einer Bildungseinrichtung verankert sein. Daraus ergibt sich eine Vielzahl an Pflichten und Aufgaben unmittelbar aus der DSGVO (Vorkehrungen zu Datenschutz und Datensicherheit; Auswahl von und Vereinbarungen mit Auftragsverarbeitern; Führung von Verarbeitungsverzeichnissen; Wahrung von Betroffenenrechten; ev. Datenschutz-Folgenabschätzungen; uvm.), die von jedem Leiter bzw. jeder Leiterin zu beachten und wahrzunehmen sind. Da gerade im Bundesschulbereich Datenverarbeitungen im Rahmen zentral vorgegebener Anwendungen (Sokrates, Web-Untis etc.) erfolgen, soll in solchen Fällen und unter bestimmten Umständen eine gemeinsame Verantwortlichkeit der „verantwortlichen" Leiterinnen und Leiter" sowie des zuständigen Bundesministers oder der zuständigen Bundesministerin vorgesehen sein.

Die Legaldefinition des für die Verarbeitung Verantwortlichen in Art. 4 Z 7 DSGVO sieht vor, dass Zweck und Mittel einer Verarbeitung nicht nur von einem Verantwortlichen bestimmt werden können, sondern dies auch mehreren Verantwortlichen gemeinsam möglich ist. Art. 26 Abs. 1 DSGVO führt dazu Folgendes aus: *„[…] Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche […]"*. Die Einführung einer elektronischen Schülerverwaltung im Bundesschulbereich, durch die eine administrative Entlastung an den Schulstandorten sowie der Einsatz modernster Technologie und einer zeitgemäßen IT-Systemstruktur ermöglicht wurde, stellt eine solche Entscheidung (im Sinne einer gemeinsamen Festlegung) über Zwecke der und Mittel zur Datenverarbeitung durch die Schulleiterinnen bzw. Schulleiter und den zuständigen Bundesminister bzw. die zuständige Bundesministerin dar. Liegt eine gemeinsame Verantwortlichkeit der Schulleiterinnen und Schulleiter und des zuständigen Bundesministers oder der zuständigen Bundesministerin vor, sind die jeweiligen (sich aus der DSGVO ergebenden) Verpflichtungen der gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 zweiter Satz DSGVO in transparenter Form in einer Vereinbarung festzulegen. Die jeweiligen Verpflichtungen bedürfen keiner Vereinbarung, *„[…] sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. […]"*. Von dieser in der DSGVO vorgesehen Möglichkeit, eine Aufgabenfestlegung schon im Gesetz festzulegen, soll bei einer gemeinsamen Verantwortlichkeit dahingehend Gebrauch gemacht werden, dass in all jenen Fällen, in denen Verarbeitungen oder Verarbeitungsschritte von Gesetzes wegen oder vom zuständigen Bundesminister oder von der zuständigen Bundesministerin vorgegeben werden, diesem bzw. dieser jedenfalls die Führung von Verzeichnissen von Verarbeitungstätigkeiten (Art. 30 DSGVO) und die Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO), sofern solche notwendig sind, zukommen soll. Hinsichtlich der übrigen nicht zugewiesenen Verpflichtungen wird eine transparente Vereinbarung abzuschließen sein.

Zu Art. 50 Z 13 (§ 3 Abs. 1):

Die Änderung des § 3 Abs. 1 stellt keine inhaltliche Neuerung dar, sondern nur eine Konkretisierung des Begriffes „hochschulrechtliche Vorschriften", indem explizit die in § 2 Abs. 2 aufgelisteten Materiengesetze in die Aufzählung in diesem Absatz aufgenommen werden.

Zu Art. 50 Z 14 (§ 3 Abs. 3 Z 8):

Hier erfolgt die Bereinigung eines redaktionellen Versehens.

Zu Art. 50 Z 15 (§ 5 Abs. 1):

Die vorgeschlagene Änderung stellt eine notwendige Anpassung an die Terminologie der DSGVO dar.Verantwortlicher (vormals Auftraggeber) der Gesamtevidenzen ist der Bundesminister oder die Bundesministerin für Bildung, Wissenschaft und Forschung.

Zu Art. 50 Z 16 (§ 5 Abs. 2):

In § 5 Abs. 2 sollen vorwiegend notwendige terminologische Anpassungen in Zusammenhang mit dem neuen Datenschutzregime der DSGVO erfolgen. Der erste Satz des Abs. 2, wonach in den Gesamtevidenzen der Schülerinnen und Schüler bzw. Studierenden nur indirekt personenbezogene Daten iSd § 4 Z 1 DSG 2000 (die Identität des Betroffenen lässt sich mit rechtlich zulässigen Mitteln nicht bestimmen) gespeichert werden dürfen, soll entfallen, da sich der Begriff „indirekt personenbezogene Daten“ in der DSGVO nicht findet.

Hinsichtlich der in der Gesamtevidenz der Schülerinnen und Schüler, die direkt beim zuständigen Bundesminister bzw. bei der zuständigen Bundesministerin geführt wird, gespeicherten Daten lässt sich grob folgender Übermittlungsweg skizzieren: Schulen übermitteln aus ihrer lokalen Evidenz (§ 3) personenbezogene Daten (bereinigt um Name, Teile der Adresse, Religionsbekenntnis etc.) an die Bundesanstalt Statistik Österreich. Diese verschlüsselt nicht rückführbar die Sozialversicherungsnummer in das Bildungsevidenzkennzeichen (BEKZ) und übermittelt, wiederum bereinigt um den Tag der Geburt und das allfällige bildungseinrichtungsspezifische Personenkennzeichen, den Datensatz an den zuständigen Bundesminister bzw. die zuständige Bundesministerin. Für den zuständigen Bundesminister bzw. die zuständige Bundesministerin handelt es sich dabei um anonyme Daten, da ohne massive rechtsmissbräuchliche Handlungen sowohl seitens des Bundesministeriums als auch seitens der Bundesanstalt Statistik Österreich kein Personenbezug mehr hergestellt werden kann. Daher war die Zuordnung in der Systematik des DSG 2000 als indirekt personenbezogene Daten zutreffend. Ein Personenbezug im Sinne der DSGVO wird vor allem im Hinblick auf die indirekte Identifizierbarkeit von Personen, die, wenn auch unter großem Aufwand, vor allem für Dritte möglich sein wird, vorliegen. Diesbezüglich sei auf den Erwägungsgrund 26 zu Art. 4 Z 1 DSGVO verwiesen, der bei der Prüfung, ob eine natürliche Person identifizierbar ist, vorsieht, dass „alle Mittel berücksichtigt werden [sollten], die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“.

Die Übermittlung an die Gesamtevidenzen durch andere geeignete Einrichtungen (zB die BRZ GmbH) als die Bundesanstalt Statistik Österreich ist derzeit nur für die in § 2 Abs. 1 Z 2 lit. a, c und f genannten postsekundären Bildungseinrichtungen vorgesehen. Dies soll künftig auch für die Pädagogischen Hochschulen (§ 2 Abs. 1 Z 2 lit. b) möglich sein. Der Verweis auf Anforderungen an die Datensicherheit, die solche Einrichtungen erfüllen müssen, soll sich künftig auf die hiefür einschlägige Bestimmung des Art. 32 DSGVO beziehen.

Zu Art. 50 Z 17 (§ 7 Abs. 1):

Die vorgeschlagene Änderung stellt einerseits eine notwendige Anpassung an die Terminologie der Datenschutz-Grundverordnung dar und bildet andererseits die Grundlage für die Verarbeitung von personenbezogenen Daten und sonstigen Informationen in den Gesamtevidenzen der Studierenden durch die Bundesministerin oder den Bundesminister.

Zu Art. 50 Z 18 (§ 7 Abs. 2):

Aufgenommen wird in die Aufzählung jener Daten, welche von den Leiterinnen und Leitern einer Bildungseinrichtung gemäß Abs. 1 an die Bundesministerin oder den Bundesminister zu übermitteln sind, auch das bereichsspezifische Personenkennzeichen BF. Das bereichsspezifische Personenkennzeichen BF soll in Hinkunft das „führende“ Datum in der Verarbeitung von Studierendendaten in den Gesamtevidenzen der Studierenden darstellen. Einerseits ist sowohl die Eindeutigkeit der Identität gewährleistet (§ 2 Z 8 E-GovG), andererseits wird damit auch eine Pseudonymisierung gemäß Art. 4 Z 5 DSGVO vorgenommen (vormals sogenannte indirekt personenbezogene Daten, DSK 22.05.2013, K202.1126/0012-DSK/2013). Für die Fachhochschulen und Fachhochschul-Studiengänge ist die Datenübermittlung an die Gesamtevidenz schon bisher und auch weiterhin im Wege der Agentur für Qualitätssicherung und Akkreditierung vorgesehen (§ 7 Abs. 2 letzter Satz). An dieser Stelle darf dazu klarstellend angemerkt werden, dass die Eingabe, Verarbeitung und Übermittlung in einer gesonderten Applikation (Bildungsinformation, BIS-FH) erfolgt.

Zu Art. 50 Z 19 (§ 7 Abs. 4):

Aufgenommen wird eine Bestimmung, welche die Datenübermittlung der Privatuniversitäten an die Bundesministerin oder den Bundesminister regelt.

Zu Art. 50 Z 20, 21, 22, 23, 24, 25, 26, 27, 28, 29 und 49 (Überschrift des § 7a sowie § 7a Abs. 1, 2, 3, 4, 5, 8, 8a, 9, 10 und 11, Anlage 3 – Datenverbund der Universitäten und Hochschulen):

Die vorgeschlagenen Änderungen in § 7a stellen überwiegend notwendige Anpassungen an die Terminologie der DSGVO dar.

1. **Anpassungen** im Zusammenhang mit der DSGVO:

Abs. 1, 2 und 10:

Da der DSGVO ein Informationsverbundsystem im Sinne des § 4 Z 13 iVm § 50 DSG 2000 fremd ist, sind hier Anpassungen vorzunehmen. Ein Informationsverbundsystem lag nach bisheriger Rechtslage vor, wenn mehrere Auftraggeber die von ihnen verarbeiteten Daten in ein gemeinsames System einspeisten und jeder Auftraggeber Zugriff auf sämtliche in diesem System verarbeiteten Daten hatte. Die Weiterführung des Datenverbundes der Universitäten und Pädagogischen Hochschulen, erweitert um die Fachhochschulen und Fachhochschul-Studiengänge sowie die Privatuniversitäten, soll nunmehr über die in Art. 26 DSGVO vorgesehene „gemeinsame Verantwortlichkeit“ der beteiligten postsekundären Bildungseinrichtungen ermöglicht werden. Im Sinne der Rechtssicherheit soll – wie bereits in § 2 Abs. 3 in der Fassung des vorliegenden Entwurfs festgelegt – nicht die Bildungseinrichtung selbst, sondern ausdrücklich die jeweilige Leiterin oder der jeweilige Leiter (bei Fachhochschulen der Erhalter) gemäß § 2 Abs. 1 Z 5 als Verantwortlicher im Sinne der DSGVO festgelegt werden. Für diese gelten sämtliche Pflichten aufgrund der DSGVO, wie auch solche hinsichtlich des Datenschutzes durch Technikgestaltung (Art. 25) und der Datensicherheit (Art. 32) unmittelbar. Die Pflichtenzuweisung an die jeweiligen gemeinsam Verantwortlichen hat in transparenter Form in einer Vereinbarung zwischen den Verantwortlichen zu erfolgen. Als Auftragsverarbeiter (bisher Dienstleister) des Datenverbundes im Sinne des Art. 4 Z8 DSGVO ist weiterhin die BRZ vorgesehen. Auch für die BRZ gelten sämtliche Pflichten aufgrund der DSGVO, wie auch solche hinsichtlich des Datenschutzes durch Technikgestaltung (Art. 25) und der Datensicherheit (Art. 32), unmittelbar.

Abs. 4 und 11:

Da die Daten von den gemeinsam Verantwortlichen im Sinne des Art. 26 DSGVO im Datenverbund verarbeitet werden, soll der Begriff des „Überlassens“ von Daten im Sinne des § 4 Z 12 DSG 2000 an die Begrifflichkeit der DSGVO angepasst und durch den Begriff „Verarbeitung“ ersetzt werden.

2. **Erweiterung des Datenverbundes** der Universitäten und der Pädagogischen Hochschulen um Fachhochschul-Studiengänge und Fachhochschulen sowie Privatuniversitäten:

Die zweite große Änderung des § 7a ist bedingt durch die geplante Einbindung der Erhalter von Fachhochschul-Studiengängen und der Privatuniversitäten in den Datenverbund, aufgrund der Ausweitung des Matrikelnummernsystems von den Universitäten und Pädagogischen Hochschulen auf die Erhalter von Fachhochschul-Studiengängen und die Privatuniversitäten.

Universitäten und Pädagogische Hochschulen verwenden schon derzeit das gleiche Matrikelnummernsystem. Ausgelöst durch die gemeinsam eingerichteten Lehramtsstudien mussten die Matrikelnummern gegenseitig übernommen werden. Voraussetzung dafür war eine eindeutige „Personen-ID“ und damit auch die Anbindung der Pädagogischen Hochschulen an den Datenverbund der Universitäten. Erhalter von Fachhochschul-Studiengängen und Privatuniversitäten verwenden derzeit andere Personen-ID-Systeme. Durch die parallel zur Begutachtung stehenden Änderungen des Universitätsgesetzes 2002, des Hochschulgesetzes 2005, des Fachhochschul-Studiengesetzes und des Privatuniversitätengesetzes sollen nunmehr explizit die Vergabe von Matrikelnummern durch die Erhalter von Fachhochschul-Studiengängen und durch die Privatuniversitäten in die beiden Materiengesetze aufgenommen werden und eine verpflichtende Übernahme einer einmal vergebenen Matrikelnummer durch andere Universitäten, Pädagogische Hochschulen, Erhalter von Fachhochschul-Studiengängen und Privatuniversitäten vorgesehen werden. Damit die ordentliche Vergabe einer Matrikelnummer durch die vorhin aufgezählten Bildungseinrichtungen gewährleistet ist, ist es für diese notwendig in Erfahrung zu bringen, ob die Studienwerberin oder der Studienwerber bereits über eine Matrikelnummer verfügt. Die Prüfung des Vorhandenseins einer Matrikelnummer soll aus verwaltungsökonomischen Gründen durch eine Abfrage aus dem Datenverbund erfolgen. Ein zukünftiges, einheitliches Matrikelnummernsystem bildet auch die Grundlage für die Administration von gemeinsam eingerichteten Studien und fördert die Durchlässigkeit, Administrierbarkeit und Praktikabilität.

Durch das Bundesgesetz, mit dem das Hochschulgesetz 2005, das Schulorganisationsgesetz und das Land- und forstwirtschaftliche Bundesschulgesetz geändert werden sowie das Hochschul-Studienberechtigungsgesetz aufgehoben wird und das Universitätsgesetz 2002, das Fachhochschul-Studiengesetz, das Privatuniversitätengesetz und das Hochschul-Qualitätssicherungsgesetz geändert werden, BGBl. I Nr. 129/2017, wurden einheitliche Bestimmungen bezüglich der Einrichtung von gemeinsamen Studienprogrammen und gemeinsam eingerichteten Studien in das Universitätsgesetz 2002, das Hochschulgesetz 2005, das Fachhochschul-Studiengesetz und das Privatuniversitätengesetz aufgenommen. In den Inkrafttretensbestimmungen dieser Novellierung des Fachhochschul-Studiengesetzes und des Privatuniversitätengesetzes ist vorgesehen, dass die Teilnahme an einem gemeinsam eingerichteten Studium mit einer Universität und bzw. oder Pädagogischen Hochschule als

gleichberechtigter Partner für einen Erhalter eines Fachhochschul-Studienganges oder eine Privatuniversität nur unter den Voraussetzungen des Vorliegens eines einheitlichen Matrikelnummernsystems und der Möglichkeit des Austausches der für die Durchführung eines gemeinsam eingerichteten Studiums erforderlichen Daten möglich ist. Dadurch soll gewährleistet sein, dass eine ordnungsgemäße Verwaltung der Studierenden möglich ist. Die Daten, die an den Datenverbund für die Administration von gemeinsamen Studienprogrammen und von gemeinsam eingerichteten Studien übermittelt werden sollen, werden in der Anlage 3 explizit aufgeschlüsselt.

Aufgenommen wird ein neuer Absatz 8a, der eine Abfrageberechtigung für öffentliche Einrichtungen und Anbieter von Dienstleistungen, die Studierenden Vergünstigungen oder Ermäßigungen gewähren, vorsieht. Diese sollen die Möglichkeit erhalten, bei Vorliegen eines Antrages einer oder eines Studierenden auf eine Vergünstigung oder Ermäßigung, beim Datenverbund abzufragen, ob der Status „Studierende“ oder „Studierender“ vorliegt. Eine solche Abfrage ist vom Auftragsverarbeiter des Datenverbundes nur dann zuzulassen, wenn die Einhaltung der Datensicherheitsmaßnahmen gemäß § 8 Abs. 2 durch die öffentliche Einrichtung oder den Anbieter von Dienstleistungen nachgewiesen wird. Zur Einhaltung der Datensicherheitsmaßnahmen hat die öffentliche Einrichtung oder der Anbieter von Dienstleistungen Folgendes nachzuweisen:

- Festlegung, wer (Identität des Abfragenden) unter welchen Voraussetzungen (Bekanntgabe des Abfragezwecks) eine Abfrage durchführen darf;
- durchgeführte Belehrung der abfrageberechtigten Mitarbeiter über ihre Pflichten;
- Regelungen über die Abfrageberechtigungen und den Schutz vor Einsicht und Verwendung der Daten durch Unbefugte;
- technische oder programmgesteuerte Vorkehrungen gegen unbefugte Abfragen;
- die Vornahme von Aufzeichnungen, damit tatsächlich durchgeführte Verwendungsvorgänge im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können (Protokollierung);
- Maßnahmen zum Schutz vor unberechtigtem Zutritt zu Räumlichkeiten, von denen aus Abfragen durchgeführt werden können.

In diesem Absatz ist auch vorgesehen, dass neben den oben aufgezählten Datenschutzmaßnahmen auch ein begründetes Interesse der öffentlichen Einrichtung oder des Anbieters von Dienstleistungen an der Abfrage bestehen muss, damit diese erteilt werden kann. Ein begründetes Interesse liegt insbesondere vor, wenn zur Überprüfung einer Fahrtkostenvergünstigung eine Abfrage durch einen Verkehrsbetrieb oder zur Überprüfung eines Fahrtkostenzuschusses eine Abfrage durch eine Gebietskörperschaft vorgenommen werden soll.

Zu Art. 50 Z 32 und 50 (§ 7b, 7c, Anlage 4):

§ 7b: Austrian Higher Education Systems Network (AHESN)

Durch das Bundesgesetz, mit dem das Hochschulgesetz 2005, das Schulorganisationsgesetz und das Land- und forstwirtschaftliche Bundesschulgesetz geändert werden sowie das Hochschul-Studienberechtigungsgesetz aufgehoben wird und das Universitätsgesetz 2002, das Fachhochschul-Studiengesetz, das Privatuniversitätengesetz und das Hochschul-Qualitätssicherungsgesetz geändert werden, BGBl. I Nr. 129/2017, wurden einheitliche Bestimmungen bezüglich der Einrichtung von gemeinsamen Studienprogrammen und gemeinsam eingerichteten Studien in das Universitätsgesetz 2002, das Hochschulgesetz 2005, das Fachhochschul-Studiengesetz und das Privatuniversitätengesetz aufgenommen. In diesen Bestimmungen ist normiert, dass bei gemeinsamen Studienprogrammen die beteiligten Bildungseinrichtungen Vereinbarungen über die Durchführung, insbesondere über die Festlegung der Leistungen, die die betreffenden Studierenden an den beteiligten Bildungseinrichtungen zu erbringen haben, abzuschließen haben.

Bei gemeinsam eingerichteten Studien haben die beteiligten österreichischen postsekundären Bildungseinrichtungen eine Vereinbarung insbesondere über die Durchführung sowie die Arbeits- und die Ressourcenaufteilung zu schließen. Die Zulassung zu einem gemeinsam eingerichteten Studium darf nur an einer der beteiligten Bildungseinrichtungen nach Wahl der oder des Studierenden erfolgen. Die Rektorate der beteiligten Universitäten und öffentlichen Pädagogischen Hochschulen können durch gleichlautend zu erlassende Verordnungen bzw. die zuständigen Organe von anerkannten privaten Pädagogischen Hochschulen, Einrichtungen zur Durchführung von Fachhochschul-Studiengängen und Privatuniversitäten können durch zu veröffentlichende gleichlautende Vereinbarungen jene Bildungseinrichtung bestimmen, welche die Zulassung durchzuführen hat. Mit der Zulassung wird die

oder der Studierende auch Angehörige oder Angehöriger aller am gemeinsam eingerichteten Studium beteiligten Bildungseinrichtungen.

Mit dieser Bestimmung soll nunmehr eine, für die an einem gemeinsamen Studienprogramm oder an einem gemeinsamen eingerichteten Studium beteiligten Bildungseinrichtungen praktikable Bestimmung für die Verarbeitung von Studierendendaten und sonstigen Informationen geschaffen werden. Neben der Bestimmung des § 7a (Datenverbund) soll daher für den Bereich der Universitäten, der Universität für Weiterbildung Krems, der Pädagogischen Hochschulen, der Erhalter von Fachhochschul-Studiengängen und der Privatuniversitäten zum Zweck der Gewährleistung der ordentlichen Verwaltung und Durchführung von gemeinsamen Studienprogrammen und gemeinsam eingerichteten Studien eine eigene gesetzliche Grundlage geschaffen werden. Zur Abgrenzung bezüglich des Zweckes des Datenverbundes gemäß § 7a ist auf Folgendes hinzuweisen:

- Im „Austrian Higher Education Systems Network“ (AHESN) werden, aufgrund des Grundsatzes der Datenminimierung gemäß Artikel 5 Z 1 lit. c, mit Ausnahme der für die eindeutige Identifizierung erforderlichen Daten, nur solche Kategorien von personenbezogenen Daten und sonstigen Informationen verarbeitet, die nicht im Datenverbund gemäß § 7a verarbeitet werden.
- Die konkreten, für die Verwaltung und Durchführung eines gemeinsamen Studienprogramms oder eines gemeinsam eingerichteten Studiums erforderlichen personenbezogenen Daten und sonstigen Informationen sind von den Verantwortlichen gemeinsam festzulegen. Der Zweck der Datenverarbeitung ist klar definiert und beschränkt sich auf die Verwaltung und Durchführung von gemeinsamen Studienprogrammen und von gemeinsam eingerichteten Studien.
- Im Gegensatz zum Datenverbund gemäß § 7a wird beim AHESN keine eigene Datenbank befüllt, sondern personenbezogene Daten und sonstige Informationen „nur“ zwischen den an einem gemeinsamen Studienprogramm oder an einem gemeinsam eingerichteten Studium beteiligten Bildungseinrichtungen ausgetauscht und verarbeitet („Peer-to-Peer“-Architektur“).

§ 7c: Datenverbund der Schulen

Nach derzeit geltender Rechtslage ist ein direkter Austausch schülerbezogener Daten zwischen Schulen nicht möglich. Derzeit werden bei Schulwechsel daher die Daten an der aufnehmenden Schule auf Grund vorgelegter Zeugnisse und anderer papierbasierter Unterlagen, wie etwa des ZMR-Auszugs, jeweils neu erfasst. Diese manuelle Neuerfassung der bereits in den lokalen Evidenzen (§ 3) elektronisch vorhandenen Daten führt insbesondere beim regelmäßigen Schulwechsel zwischen 4. und 5. sowie 8. und 9. Schulstufe, aber auch beim unterjährigen Wechsel zu hohem Administrationsaufwand in den Schulen. Zugleich wird damit ein ordnungs- und gesetzmäßiger Vollzug schulrechtlicher Vorschriften erschwert.

Aus diesem Grund soll zum Zweck der Vollständigkeit und der Richtigkeit der bei der Aufnahme von Schülerinnen und Schülern in den lokalen Evidenzen zu verarbeitenden Schülerdaten ein Datenverbund der Schulen eingerichtet werden. Im Hinblick auf die unterschiedliche technische Ausstattung sowie Ausstattung mit Software im Bereich der Pflichtschulen sowie der Privatschulen soll die automationsunterstützte Dateneingabe im Schuljahr 2018/19 nur nach Maßgabe der technischen Möglichkeiten erfolgen. Wie beim Datenverbund der Universitäten und Hochschulen (§ 7a) ist datenschutzrechtlich eine „gemeinsame Verantwortlichkeit“ der Leiter bzw. Leiterinnen der beteiligten Schulen im Sinne des Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO vorgesehen. Auch beim Datenverbund der Schulen fungiert die BRZ als Auftragsverarbeiter im Sinne des Art. 4 Z 8 DSGVO.

Die im Falle eines Schulwechsels zu verarbeitenden schülerbezogenen Daten sind in Anlage 4 taxativ aufgezählt. In allen Fällen, in denen es zu einer Beendigung der Schülereigenschaft eines Schülers oder einer Schülerin an der betreffenden Schule kommt, hat die Schulleitung den Schülerdatensatz von sich aus, jedenfalls jedoch bei Anfrage durch die Schulleitung einer den betreffenden Schüler oder die betreffende Schülerin aufnehmenden Schule, dem Datenverbund zu übermitteln. Eine Abfrageberechtigung ist für Schulleitungen nur hinsichtlich der an der betreffenden Schule aufgenommenen Schülerinnen und Schüler vorgesehen. Ungeachtet des Umstandes, dass die Schulleitungen als datenschutzrechtlich Verantwortliche ausreichende Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO zu treffen haben, darf eine Abfrage durch die BRZ nur bei Nachweis der in § 8 Abs. 2 vorgesehen Datensicherheitsmaßnahmen zugelassen werden. Weiters ist die Abfrage seitens der BRZ so einzurichten, dass nur unter der Verwendung von Antragsdaten nach den jeweiligen gesetzlichen Bestimmungen auf die Daten von Schülerinnen und Schülern zugegriffen werden kann. Nach erfolgter Abfrage des Schülerdatensatzes ist dieser aus dem Datenverbund zu löschen. Durch geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO ist sicherzustellen, dass der Datenverbund der Schulen ausschließlich als „Datendrehscheibe“ unmittelbar im Zuge des Schulwechsels verwendet werden kann. Wie auch beim Datenverbund im Universitäts- und Hochschulbereich sind die näheren Bestimmungen zu den Stichtagen, Verfahren und Formaten der Datenverarbeitung, zum

Verfahren der Übermittlung von Daten an die abfrageberechtigten Einrichtungen sowie zu den Datensicherheitsmaßnahmen durch Verordnung der zuständigen Bundesministerin bzw. des zuständigen Bundesministers zu regeln.

Zu Art. 50 Z 31 (§ 8 Abs. 1 und 2):

Hier erfolgen Anpassungen an die geänderten Ressortbezeichnungen gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 50 Z 32, 33, 34 und 35 (§ 8 Abs. 1, Abs. 2 und Abs. 3 Z 2):

Die vorgenommenen Änderungen betreffen terminologische Anpassungen an die DSGVO. Hinsichtlich der Datensicherheitsmaßnahmen in § 8 Abs. 1 soll künftig auf Art. 32 DSGVO verwiesen werden. Die Pflichten Verantwortlicher und Auftragsverarbeiter hinsichtlich zu treffender Datenschutz- und Datensicherheitsmaßnahmen ergeben sich unmittelbar aus den Bestimmungen der DSGVO (neben Art. 32 sind dies Art. 24 und 25 für Verantwortliche bzw. Art. 25 für Auftragsverarbeiter). Diese Pflichten sollen jedoch ebenso für Abfragewerber aus den Gesamtevidenzen als Voraussetzung für die Erteilung einer Abfrageberechtigung vorgesehen sein. Die gesonderte Aufzählung von Datensicherheitsmaßnahmen, die durch Verordnung des zuständigen Bundesministers oder der zuständigen Bundesministerin näher auszugestalten sind, soll bestehen bleiben. Dies ist weder als Einschränkung noch als Ausgestaltung der unmittelbar anzuwendenden Bestimmungen der DSGVO zu verstehen.

Zu Art. 50 Z 36 (Entfall des § 8 Abs. 4):

Die Nennung von Auskunftsrechten bei der Verarbeitung personenbezogener Daten in den lokalen Evidenzen soll im Hinblick auf die unmittelbare Geltung der DSGVO bezüglich der Rechte betroffener Personen (ua. Art. 15, 16 DSGVO) entfallen.

Zu Art. 50 Z 37 (§ 9 Abs. 2 Z 1 lit. b):

Hier erfolgt die Bereinigung eines redaktionellen Versehens.

Zu Art. 50 Z 38 (§ 10 Abs. 3 Z 2):

Der Verweis auf das Anerkennungs- und Bewertungsgesetz soll entfallen, da er in der Praxis bei der Erhebung zu Interpretationsschwierigkeiten hinsichtlich der Meldungen von Anerkennungen der Bildungsabschlüsse von Elementarpädagoginnen und –pädagogen aus der EU führt.

Zu Art. 50 Z 39 und 40 (Überschrift zu § 10a und § 10a Abs. 2):

Es sollen notwendige Anpassungen an die Terminologie der DSGVO vorgenommen werden.

Zu Art. 50 Z 41 (§ 10a Abs. 3):

Nach Erstellung der Bundesstatistik zum Bildungswesen und der Bildungsstandstatistik sind die Sozialversicherungsnummern von der Bundesanstalt „Statistik Österreich“ gemäß § 15 des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999, zu verschlüsseln. Da in § 15 des Bundesstatistikgesetzes 2000 von der Öffnungsklausel des Art. 89 Abs. 2 DSGVO, wonach bei der Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken die Betroffenenrechte gemäß Art. 15, 16, 18 und 21 ausgeschlossen werden können, Gebrauch gemacht werden soll, wird diese Änderung auch hier nachvollzogen. Die Betroffenenrechte sollen jedoch nur insofern beschränkt werden, als dadurch die Verarbeitung dieser Daten für statistische Zwecke erheblich beeinträchtigt oder unmöglich gemacht würde.“

Zu Art. 50 Z 42 (§ 11 Abs. 5):

Der Verweis auf § 4 Z 1 DSG 2000 betreffend die Begriffsbestimmung personenbezogener Daten soll durch einen Verweis auf Art. 4 Z 1 DSGVO ersetzt werden.

Zu Art. 50 Z 43 (§ 12 Abs. 19):

Diese Bestimmung regelt das Inkrafttreten wie folgt:

Hinsichtlich der Änderungen der Ressortbezeichnung aufgrund der Bundesministeriengesetz-Novelle 2017, der Regelungen zum Datenverbund der Universitäten und Hochschulen, die sich auf die Einbeziehung der Fachhochschulen und Fachhochschul-Studiengänge sowie der Privatuniversitäten beziehen, der gesetzlichen Verankerung des „Austrian Higher Education Systems Network“ sowie hinsichtlich sonstiger rein redaktioneller Änderungen ist das Inkrafttreten mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt vorgesehen. Die datenschutzrechtlich relevanten Änderungen sollen in Übereinstimmung mit dem Wirksamwerden der DSGVO mit 25. Mai 2018 in Kraft treten. Schließlich sollen die Regelungen zum Datenverbund der Schulen mit 1. September 2018 in Kraft gesetzt werden, um im Schuljahr 2018/2019 zur Anwendung gelangen zu können.

Zu Art. 50 Z 44 (§ 14 Abs. 7):

An dieser Stelle soll eine Übergangsbestimmung betreffend die Fachhochschulen und Fachhochschul-Studiengänge sowie die Privatuniversitäten im Hinblick auf die Einbeziehung in den Datenverbund der Universitäten und Hochschulen eingefügt werden.

Die Fachhochschulen und Fachhochschul-Studiengänge sowie die Privatuniversitäten haben sicherzustellen, dass die Teilnahme am Datenverbund im Bereich der Studierendendaten und der Vergabe von Matrikelnummern für das Wintersemester 2018/19 umgesetzt wird. Die Integration der Studiendaten hat für Fachhochschulen und Fachhochschul-Studiengänge beginnend ab dem Wintersemester 2019/20 zu erfolgen.

Zu Art. 50 Z 45 (§ 15):

Hier erfolgt eine Neufassung der Vollzugsbestimmung aufgrund der geänderten Ressortzuständigkeiten gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 50 Z 46 und 47 (Anlage 1 Z 1,1a und 9):

In den lokalen Evidenzen (§ 3) sind nach Maßgabe der Anlage 1 auch Daten über den Bildungsverlauf der Schülerinnen und Schüler zu verarbeiten. Diese Informationen finden gemäß § 6 Abs. 2 Z 2 auch in die Gesamtevidenzen der Schülerinnen und Schüler Eingang. Der Z 1 (diese wird in Z 1a umbenannt) soll eine neue Ziffer vorangestellt werden, dergemäß auch Daten über den Bildungsverlauf vor Beginn der allgemeinen Schulpflicht zu erfassen sind. Im Besonderen (näher auszuführen in der Anlage zur Bildungsdokumentationsverordnung) wird es um die Zahl der Kindergartenjahre und um besondere (Sprach)Förderungen im Vorschulalter gehen, die gemäß der neuen Z 1 zu verarbeiten sind. Diese Informationen werden gemäß § 6 Abs. 1a Schulpflichtgesetz 1985 von den Erziehungsberechtigten zur Verfügung gestellt oder – siehe die genannte Bestimmung im vorliegenden Entwurf – nach Maßgabe landesgesetzlicher Bestimmungen vom Kindergarten automationsunterstützt übermittelt. Die Z 9 in Anlage 1 ist aufgrund der Zusammenfassung der getrennten Pflichtgegenstände bzw. alternativen Pflichtgegenstände „Technisches Werken“ und „Textiles Werken“ zu einem Pflichtgegenstand „Technisches und textiles Werken“ obsolet und kann daher entfallen.

Zu Art. 50 Z 48 (Anlage 1 Z 14):

Hier soll der ins Leere gehende Verweis auf § 24a des Schulpflichtgesetzes 1985 entfallen und die Ziffer neu gefasst werden. Diese Informationen sind gemäß § 7c und der Anlage 4 des Entwurfs (siehe die Ausführungen zu Z 32 und 5) im Datenverbund der Schulen zur Verfügung zu stellen, damit im Fall des Schulwechsels der Leiter oder die Leiterin der aufnehmenden Schule über allfällige Maßnahmen im Zusammenhang mit Schulpflichtverletzungen Bescheid weiß (zB Verwarnungen wegen unentschuldigtem Fernbleiben oder Strafanzeigen wegen Schulpflichtverletzungen).

Zu Art. 51 (Änderung des Schulunterrichtsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 1 B-VG (Schulwesen).

Zu Art. 51 Z 1, 2 und 3 (§ 57b Abs. 1 und 2; Entfall des § 57b Abs. 3):

Schülerinnen- bzw. Schülerkarten können freiwillig beantragt werden und dienen dem Nachweis der Eigenschaft als Schülerin oder Schüler an der betreffenden Schule. Sie können mit weiteren Funktionalitäten ausgestattet sein und elektronische Verknüpfungen zu anderen Dienstleistern aufweisen (zB für bargeldloses Zahlen). Dies erfordert die schriftliche Zustimmung der Schülerin oder des Schülers oder, bei fehlender Eigenberechtigung, gemäß § 67 SchUG deren bzw. dessen Erziehungsberechtigten. Sowohl die Beantragung der Schülerinnen- bzw. Schülerkarte als auch die Zustimmung zu weiteren Funktionalitäten und elektronischen Verknüpfungen stellten bisher eine Zustimmung im Sinne des § 4 Z 14 DSG 2000 in der Fassung vor der Novelle BGBl. I Nr. 120/2017 dar. Nun soll der datenschutzrechtliche Begriff der „Zustimmung“ durch den ab 25. Mai 2018 maßgeblichen Begriff der „Einwilligung“ im Sinne des Art. 4 Z 11 DSGVO ersetzt bzw. neu eingeführt werden und Abs. 3 entfallen, da sich die Definition der Einwilligung bereits unmittelbar aus der DSGVO ergibt.

Zu Art. 51 Z 4 (§ 77 Abs. 2):

In Klassenbüchern werden unter anderem zu Dokumentations- und Beweiszwecken (ordnungsgemäßer Unterricht, besondere Vorkommnisse usw.) diverse personenbezogene Daten vermerkt. Die Dokumentation besonders schutzwürdiger Daten („sensible“ Daten im Sinne des § 4 Z 2 DSG 2000) im Klassenbuch ist dann zulässig, wenn diese der Wahrung eines wichtigen öffentlichen Interesses im Sinne

des § 9 Z 3 DSG 2000 dient. Diesbezüglich soll eine Anpassung an die DSGVO dahingehend erfolgen, dass die Begriffsbestimmung angepasst wird („Besondere Kategorien personenbezogener Daten“) und auf die betreffende Bestimmung der DSGVO verwiesen wird (Art. 9 Abs. 1). Weiters ist zu berücksichtigen, dass die Dokumentation solcher Daten für die Erreichung der in Abs. 1 festgelegten Zwecke gemäß Art. 9 Abs. 2 lit. g DSGVO ein „erhebliches“ statt wie bisher „wichtiges“ öffentliches Interesse darstellen muss.

Zu Art. 51 Z 5 (§ 77 Abs. 3):

Hinsichtlich der zu treffenden Datensicherheitsmaßnahmen wird aufgrund der unmittelbaren Geltung der DSGVO auf deren Art. 32 verwiesen. In der DSGVO wurden keine Regelungen zum Datengeheimnis vorgesehen, eine entsprechende Bestimmung findet sich jedoch weiterhin im DSG (§ 6 DSG – vormals § 15 DSG 2000), auf das daher verwiesen werden soll.

Zu Art. 51 Z 6 (§ 82 Abs. 10):

Diese Bestimmung regelt das Inkrafttreten in Übereinstimmung mit dem Wirksamwerden der DSGVO sowie dem Inkrafttreten der maßgeblichen Änderungen des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, mit 25. Mai 2018.

Zu Art. 52 (Änderung des Schulunterrichtsgesetzes für Berufstätige, Kollegs und Vorbereitungslehrgänge)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 1 B-VG (Schulwesen).

Zu Art. 52 Z 1, 2 und 3 (§ 55a Abs. 1 und 2; Entfall des § 55a Abs. 3):

Analog zur Änderung des § 57b SchUG (siehe die Erläuterungen zu Art. 51 Z 1 bis 3 des gegenständlichen Entwurfs) soll auch hier der datenschutzrechtliche Begriff der „Zustimmung“ durch den ab 25. Mai 2018 maßgeblichen Begriff der „Einwilligung“ im Sinne des Art. 4 Z 11 DSGVO ersetzt bzw. neu eingeführt werden und Abs. 3 entfallen, da sich die Definition der Einwilligung bereits unmittelbar aus der DSGVO ergibt.

Zu Art. 52 Z 4 (§ 65 Abs. 2):

In Klassenbüchern werden unter anderem zu Dokumentations- und Beweiszwecken (ordnungsgemäßer Unterrichts, besondere Vorkommnisse usw.) diverse personenbezogene Daten vermerkt. Die Dokumentation besonders schutzwürdiger Daten („sensible“ Daten im Sinne des § 4 Z 2 DSG 2000) im Klassenbuch ist dann zulässig, wenn diese der Wahrung eines wichtigen öffentlichen Interesses im Sinne des § 9 Z 3 DSG 2000 dient. Diesbezüglich soll eine Anpassung an die DSGVO dahingehend erfolgen, dass die Begriffsbestimmung angepasst wird („Besondere Kategorien personenbezogener Daten“) und auf die betreffende Bestimmung der DSGVO verwiesen wird (Art. 9 Abs. 1). Weiters ist zu berücksichtigen, dass die Dokumentation solcher Daten für die Erreichung der in Abs. 1 festgelegten Zwecke gemäß Art. 9 Abs. 2 lit. g DSGVO ein „erhebliches“ statt wie bisher „wichtiges“ öffentliches Interesse darstellen muss.

Zu Art. 52 Z 5 (§ 65 Abs. 3):

Hinsichtlich der zu treffenden Datensicherheitsmaßnahmen wird aufgrund der unmittelbaren Geltung der DSGVO auf deren Art. 32 verwiesen. In der DSGVO wurden keine Regelungen zum Datengeheimnis vorgesehen, eine entsprechende Bestimmung findet sich jedoch weiterhin im DSG (§ 6 DSG – vormals § 15 DSG 2000), auf das daher verwiesen werden soll.

Zu Art. 52 Z 6 (§ 69 Abs. 12):

Diese Bestimmung regelt das Inkrafttreten in Übereinstimmung mit dem Wirksamwerden der DSGVO sowie dem Inkrafttreten der maßgeblichen Änderungen des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, mit 25. Mai 2018. Die Änderungen hinsichtlich der Ressortbezeichnungen aufgrund der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, sollen sofort in Kraft treten.

Zu Art. 52 Z 7 (§ 70):

Hier erfolgen Anpassungen an die geänderten Ressortbezeichnungen gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 53 (Änderung des Schulpflichtgesetzes 1985)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 1 B-VG (Schulwesen).

Zu Art. 53 Z 1 (§ 6 Abs. 1a):

Bereits derzeit haben die Erziehungsberechtigten eines Kindes im Zuge dessen Aufnahme in die Volksschule sämtliche ihnen von der Kindergartenleitung zur Verfügung gestellten Unterlagen sowie Erhebungen und Förderergebnisse zur Dokumentation des Entwicklungsstandes, insbesondere des Sprachstandes, zur Verfügung gestellt wurden, vorzulegen. Zusätzlich soll mit der vorgeschlagenen Regelung bewirkt werden, dass im Fall der Zulässigkeit eines Datenaustausches nach landesgesetzlichen Bestimmungen über die Datenverarbeitung auch vom Kindergarten automationsunterstützt übermittelte Daten vom Schulleiter oder von der Schulleiterin erfasst und weiter verarbeitet werden dürfen. Datenverarbeitungen gemäß dieser Bestimmung (§ 6 Abs. 1a SchPflG) sind solche gemäß § 3 Abs. 2 Z 7 und Anlage 1 des Bildungsdokumentationsgesetzes (Daten über den Bildungsverlauf vor Beginn der allgemeinen Schulpflicht), sodass die Bestimmungen dieses Bundesgesetzes zur Anwendung kommen und vor allem die datenschutzrechtlichen Details dieser Verarbeitungen im Schulpflichtgesetz 1985 nicht nochmals geregelt werden müssen. Es handelt sich jedenfalls um personenbezogene Daten im Sinne des Art. 4 Z 1 der Datenschutz-Grundverordnung. Auf die Ausführungen zu Z 47 des im vorliegenden Gesetzesvorschlags sei verwiesen.

Zu Art. 53 Z 2 und 3 (§ 16 Abs. 1 und 5):

Mit dem Bildungsreformgesetz 2017, BGBl. I Nr. 138/2017, wurde die Schulpflichtmatrik, die der Überprüfung der Erfüllung der allgemeinen Schulpflicht dient, neu geregelt.

Die Begründung zum Initiativantrag 2254/A 25. GP führt dazu aus:

„Dies soll in der Weise geschehen, dass die Bundesrechenzentrum GmbH als IT-Dienstleisterin der Bildungsdirektionen bestimmte gemäß Bildungsdokumentationsgesetz verfügbare Daten (im Detail siehe den Entwurf) mit bestimmten Daten (im Detail siehe den Entwurf), die der Bundesminister für Inneres aus dem Datenbestand des zentralen Melderegisters zur Verfügung stellt, automationsunterstützt abgleicht. Übereinstimmende Datensätze sind unverzüglich zu löschen. Nur diejenigen Datensätze, denen zufolge nach Meldegesetz gemeldete Personen in schulischen Meldungen nicht aufscheinen, sind der Bildungsdirektion zu übermitteln. Diese hat sodann für die Erfüllung der Schulpflicht durch die betroffene Person Vorkehrungen zu treffen, allenfalls (als letzten Schritt) Strafverfahren einzuleiten.“

Bei den Änderungen handelt es sich um notwendige terminologische Anpassungen an die DSGVO. So soll der Begriff „IT-Dienstleister“ durch den Begriff „Auftragsverarbeiter“ ersetzt und auf Art. 4 Z 8 DSGVO verwiesen werden.

Zu Art. 53 Z 4 (§ 30 Abs. 22):

§ 6 Abs. 1b soll mit Beginn des Schuljahres 2018/19 in Kraft treten.

Da das Inkrafttreten des § 16 in der Fassung des Bildungsreformgesetzes 2017 erst mit 1. September 2019 vorgesehen ist, sollen auch die jetzigen Änderungen erst zu diesem Zeitpunkt in Kraft treten und an die Stelle der ursprünglichen Regelung treten (lex posterior derogat legi priori).

Zu Art. 54 (Änderung des BIFIE-Gesetzes 2008)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 13 B-VG, Art. 14 Abs. 1 B-VG und Art. 14a Abs. 2 B-VG.

Zu Art. 54 Z 1 (§ 3 Abs. 3):

Hier soll die Anwendbarkeit des 1. und 2. Abschnitts des Forschungsorganisationsgesetzes, BGBl. Nr. 341/1981, auch im Anwendungsbereich des BIFIE-Gesetzes 2008 vorgesehen werden, soweit dieses keine abweichenden Bestimmungen enthält. Die zukünftige Anwendbarkeit des wissenschaftlichen Sonderdatenschutzrechts ergibt sich zwar bereits aus § 1 Abs. 1 Z 1 des Forschungsorganisationsgesetzes in der Fassung eines parallel geplanten Datenschutz-Anpassungsgesetzes für den Bereich der Wissenschaft und Forschung, wonach allgemeine Angelegenheiten der Tätigkeiten zu Zwecken gemäß Art. 89 Abs. 1 DSGVO sowie der Verarbeitung von Daten, soweit diese für Zwecke gemäß Art. 89 DSGVO erfolgt, Gegenstand des Forschungsorganisationsgesetzes sind. Allerdings soll aus Gründen der

Rechtssicherheit durch den neu eingefügten Abs. 3 klargestellt werden, dass die Spezialbestimmungen des 1. und 2. Abschnitts des Forschungsorganisationsgesetzes jedenfalls auch für das BIFIE gelten.

Zu Art. 54 Z 2 (§ 6 Abs. 2 und 3):

Gemäß § 6 Abs. 2 des BIFIE-Gesetzes 2008 in der Fassung vor der Novelle BGBl. I Nr. 138/2017 ist bzw. war die Mitwirkung an anderen Erhebungen als an Überprüfungen der Bildungsstandards sowie an nationalen und internationalen Surveys oder Assessments für Schülerinnen und Schüler nur dann verpflichtend, wenn dies durch Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung angeordnet wird bzw. wurde (sog. BIFIE-Erhebungsverordnungen: zuletzt mit BGBl. II Nr. 113/2017). Mit dem Bildungsreformgesetz 2017 wurde eine ab dem Jahr 2019 geltende eigene gesetzliche Grundlage in § 6 des BIFIE-Gesetzes 2008 für Kontexterhebungen und die Verpflichtung zur Teilnahme an diesen für die Schülerinnen und Schüler sowie nunmehr auch deren Erziehungsberechtigen geschaffen. Solche Kontexterhebungen über schulische und außerschulische Lern- und Lebensbedingungen (Herkunft, Berufsstand der Eltern, soziale Situation) erfolgen im öffentlichen Interesse zum Zweck der statistischen Auswertung der erhobenen Daten für mehrere Bereiche (angewandte Bildungsforschung, Bildungsmonitoring, Qualitätsentwicklung, Bildungsberichterstattung, Ressourcenbewirtschaftung etc.), aber auch zum Zweck der wissenschaftlichen Forschung. Nicht zuletzt soll die Verknüpfung und Interpretation der Testergebnisse mit schulischen (z. B. Schulklima, Schulzufriedenheit) und außerschulischen Rahmenbedingungen (Geschlecht, Migrationshintergrund, Bildungsabschlüsse der Eltern u.Ä.) die Ableitung qualitätssichernder und steuerungsrelevanter Schlussfolgerungen ermöglichen. Ein direkter Personenbezug der verarbeiteten Daten, außer hinsichtlich der Testungen durch die betroffenen Schülerinnen und Schüler selbst, durfte schon bisher nicht herstellbar sein. „Technisch“ erfolgt die Verknüpfung der eigentlichen Testungen sowie der Kontextfragebögen durch die Verwendung eines gemeinsamen Codes, sodass die verschiedenen Testteile und dazugehörigen Fragebögen als zu einer Person gehörig identifiziert werden können. Dem BIFIE ist es jedoch nicht möglich, einen Code mit einem bestimmten Schüler oder einer bestimmten Schülerin in Verbindung zu bringen. Den Schülerinnen und Schülern selbst steht ein Zugang zu ihren Testergebnissen mittels des Codes, den sie aus den Testunterlagen entfernen („heraustrennen“), zur Verfügung. Wenngleich das BIFIE als Verantwortlicher gemäß Art. 4 Z 7 DSGVO Schülerinnen und Schüler nicht mehr (direkt oder indirekt) identifizieren kann, so wird es sich unter Berücksichtigung des Erwägungsgrundes 26 bei den verarbeiteten Daten dennoch um personenbezogene, und damit vom Anwendungsbereich der DSGVO umfasste, Daten im Sinne des Art. 4 Z 1 DSGVO handeln, da die zumindest indirekte Identifizierung von Personen, wenn auch nicht mit rechtlich zulässigen Mitteln und unter großem Aufwand, vor allem für Dritte möglich sein wird. Der Erwägungsgrund 26 führt dazu Folgendes aus:

„[…] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. […]“

Für das BIFIE gelten somit bei der Datenverarbeitung sämtliche Pflichten aufgrund der DSGVO, wie auch solche hinsichtlich des Datenschutzes durch Technikgestaltung (Art. 25) und der Datensicherheit (Art. 32) unmittelbar. Die Verpflichtung, bei den durchgeführten Testungen und Erhebungen Vorkehrungen und Maßnahmen (wie zB Zutrittsbeschränkung, räumliche Abgrenzungen, Belehrung, geeignete Verschlüsselungstechniken, Pseudonymisierung) zu treffen, damit kein direkter Personenbezug hergestellt werden kann, bleibt davon unberührt und ist weder als Einschränkung noch als Ausgestaltung der Bestimmungen der DSGVO zu verstehen.

Spätestens nach Ablauf des dritten Jahres nach Durchführung der Erhebungen sind die erhobenen Daten dergestalt zu anonymisieren, dass betroffene Personen nicht mehr identifiziert werden können. Diese anonymisierten Daten unterliegen nicht mehr dem Anwendungsbereich der DSGVO.

Zu Art. 54 Z 3 (Entfall des § 7 Abs. 1a):

Die hier verwendete Begriffsbestimmung zu personenbezogenen und nicht personenbezogenen Daten, die jener des § 3 Z 15 des Bundestatistikgesetzes 2000 entspricht, weicht von der Begriffsbestimmung des Art. 4 Z 1 DSGVO ab. Da hiefür keine weitere Notwendigkeit gesehen wird und aus Gründen der Rechtssicherheit soll Abs. 1a entfallen.

Zu Art. 54 Z 4 (Entfall des § 7b Abs. 2):

Dieser Absatz kann im Sinne einer Rechtsbereinigung entfallen, da sich die Voraussetzungen für Zulässigkeit einer Datenübermittlung unmittelbar aus der DSGVO ergeben.

Zu Art. 54 Z 5 (§ 7b Abs. 3):

Die Änderung stellt eine notwendige terminologische Anpassung aufgrund der DSGVO („Dienstleister“ wird zum „Auftragsverarbeiter“) dar.

Zu Art. 54 Z 6 und 7 (§ 9 Abs. 4):

Mit den Zitatanpassungen soll ein redaktionelles Versehen behoben werden.

Zu Art. 54 Z 8, 9 und 10 (§ 9a Abs. 2 Z 3 und 5, § 11 Abs. 1 Z 3 sowie § 12 Abs. 1):

Hier erfolgen Anpassungen aufgrund der geänderten Ressortzuständigkeiten gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 54 Z 11 (§ 27):

Hier erfolgt die Neufassung der Vollzugsbestimmung aufgrund der geänderten Ressortzuständigkeiten.

Zu Art. 54 Z 12 (§ 28 Abs. 6):

Diese Bestimmung regelt das In- bzw. Außerkrafttreten wie folgt:

Die geänderten Ressortbezeichnungen und die sonstigen rein redaktionellen Änderungen können mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft treten; hinsichtlich der datenschutzrechtlich relevanten Änderungen ist das In- bzw. Außerkrafttreten in Übereinstimmung mit dem Wirksamwerden der DSGVO mit 25. Mai 2018 vorgesehen. Da das Inkrafttreten des § 6 Abs. 2 und 3 in der Fassung des Bildungsreformgesetzes 2017 erst mit 1. Jänner 2019 erfolgen soll, sollen auch die jetzigen Änderungen erst zu diesem Zeitpunkt in Kraft treten und an die Stelle der ursprünglichen Regelung treten (lex posterior derogat legi priori).

Zu Art. 55 (Änderung des Hochschulgesetzes 2005)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 1 B-VG (Schulwesen).

Zu Art. 55 Z 1 (§ 1 Abs. 3):

Hier soll die Anwendbarkeit des 1. und 2. Abschnitts des Forschungsorganisationsgesetzes, BGBl. Nr. 341/1981, auch im Anwendungsbereich des Hochschulgesetzes 2005 vorgesehen werden, soweit dieses keine abweichenden Bestimmungen enthält. Die zukünftige Anwendbarkeit des wissenschaftlichen Sonderdatenschutzrechts ergibt sich zwar bereits aus § 1 Abs. 1 Z 1 des Forschungsorganisationsgesetzes in der Fassung eines parallel geplanten Datenschutz-Anpassungsgesetzes für den Bereich der Wissenschaft und Forschung, wonach allgemeine Angelegenheiten der Tätigkeiten zu Zwecken gemäß Art. 89 Abs. 1 DSGVO sowie der Verarbeitung von Daten, soweit diese für Zwecke gemäß Art. 89 DSGVO erfolgt, Gegenstand des Forschungsorganisationsgesetzes sind. Allerdings soll aus Gründen der Rechtssicherheit durch den neu eingefügten Abs. 3 klargestellt werden, dass die Spezialbestimmungen des 1. und 2. Abschnitts des Forschungsorganisationsgesetzes jedenfalls auch für die Pädagogischen Hochschulen gelten.

Zu Art. 55 Z 1, 2 (§ 12 Abs. 1 Z 1 sowie Abs. 2 Z 1 und 2, § 17 Abs. 3):

Hier erfolgen Anpassungen aufgrund der geänderten Ressortbezeichnungen gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 55 Z 4 und 6 (§ 21 Abs. 5, § 33 Abs. 3):

In § 21 Abs. 5 wird eine terminologische Anpassung an die DSGVO für die Begriffe „aufgezeichneten“, „Genehmigung“ und „Betroffene“ vorgenommen und diese in „verarbeiteten“ (Art. 4 Z 2), „Einwilligung“ (Art. 4 Z 11) und „betroffene Personen“ geändert. In § 33 Abs. 3 soll durch den Klammerausdruck klargestellt werden, dass sowohl personenbezogene Daten (Art. 4 Z 1 DSGVO) als auch nicht personenbezogene Daten umfasst sind.

Zu Art. 55 Z 5 (§ 24 Abs. 3):

Aufgrund der Änderung der Ressortzuständigkeiten gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, ist bei Ausübung des Aufsichtsrechts bei gemeinsam eingerichteten Studien unter Beteiligung von Universitäten und Pädagogischen Hochschulen mit einer Ausnahme kein Einvernehmen

zwischen den zuständigen Bundesministerinnen bzw. Bundesministern notwendig. Die Ausnahme betrifft gemeinsam eingerichtete Studien unter Beteiligung der Hochschule für Agrar- und Umweltpädagogik Wien, wo weiterhin die Bundesministerin oder der Bundesminister für Nachhaltigkeit und Tourismus das Einvernehmen mit der Bundesministerin oder dem Bundesminister für Bildung, Wissenschaft und Forschung herzustellen hat.

Zu Art. 55 Z 7, 8, 9, 11 und 12 (§ 52d Abs. 3, § 53 Abs. 1, § 65 Abs. 7, § 69 Abs. 6, § 71 Abs. 6):

Bei all jenen Bestimmungen, die eine gemeinsame Verordnung des Bundesministers oder der Bundesministerin für Bildung und des Bundesministers oder der Bundesministerin für Wissenschaft, Forschung und Wirtschaft vorsehen, ist infolge der geänderten Ressortzuständigkeiten gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, künftig eine Verordnung des Bundesministers oder der Bundesministerin für Bildung, Wissenschaft und Forschung zu erlassen.

Zu Art. 55 Z 8 (§ 53 Abs. 1):

Universitäten und Pädagogische Hochschulen verwenden das gleiche Matrikelnummernsystem. Ausgelöst durch die gemeinsam eingerichteten Lehramtsstudien mussten die Matrikelnummern gegenseitig übernommen werden. Voraussetzung dafür war eine eindeutige „Personen-ID“ und damit auch die Anbindung der Pädagogischen Hochschulen an den Datenverbund der Universitäten. Erhalter von Fachhochschul-Studiengängen und Privatuniversitäten verwenden derzeit andere Personen-ID-Systeme. Durch die vorgeschlagene Änderung zu sollen nunmehr auch die Erhalter von Fachhochschul-Studiengängen und Privatuniversitäten in ein einheitliches Matrikelnummernsystem einbezogen werden. Dies bedingt auch die Einbeziehung in den Datenverbund der Universitäten und Pädagogischen Hochschulen (künftig als Datenverbund der Universitäten und Hochschulen), was durch eine Novellierung des Bildungsdokumentationsgesetzes (Art. 50 Z 20 des vorliegenden Gesetzesvorschlags) erfolgen soll. Ein zukünftiges, einheitliches Matrikelnummernsystem bildet die Grundlage für die Administration von gemeinsam eingerichteten Studien und fördert die Durchlässigkeit, Administrierbarkeit und Praktikabilität.

Zu Art. 55 Z 10 (§ 69 Abs. 1):

Hier erfolgt die Bereinigung eines redaktionellen Versehens.

Zu Art. 55 Z 13, 14, 15, 16 und 19 (§ 74a Abs. 1, 2, 6 und 8; Anlage zu § 74a Abs. 1 Z 4):

Für Angelegenheiten betreffend den Qualitätssicherungsrat ist nach der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, der Bundesminister oder die Bundesministerin für Bildung, Wissenschaft und Forschung zuständig. In diesem Zusammenhang sind Anpassungen (Einrichtung, Bestellung von Mitgliedern etc.) vorzunehmen.

Zu Art. 55 Z 17 (§ 79):

Die Vollzugsbestimmung des § 79 soll aufgrund der geänderten Ressortzuständigkeiten gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, neu gefasst werden.

Zu Art. 55 Z 18 (§ 80 Abs. 14):

Diese Bestimmung regelt das Inkrafttreten, das hinsichtlich der datenschutzrechtlich relevanten Änderungen in Übereinstimmung mit dem Wirksamwerden der DSGVO mit 25. Mai 2018, hinsichtlich der geänderten Ressortbezeichnungen und sonstigen rein redaktionellen Änderungen mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt vorgesehen ist.

Zu Art. 56 (Änderung des Schülerbeihilfengesetzes 1983)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 14 Abs. 1 B-VG (Schulwesen).

Zu Art. 56 Z 1 (§ 1a Z 4):

Hier soll eine redaktionelle Ergänzung (in Anlehnung an die Begriffsbestimmung im Asylgesetz 2005) hinsichtlich der „Genfer Flüchtlingskonvention“ in der durch das Protokoll über die Rechtsstellung der Flüchtlinge vom 31. Jänner 1967, BGBl. Nr. 78/1974, geänderten Fassung erfolgen.

Zu Art. 56 Z 2 und 3 (§ 13 Z 1):

Hier erfolgt eine Anpassung aufgrund der geänderten Ressortbezeichnungen gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

Zu Art. 56 Z 4 (Schlusssatz des § 13):

Die in Beihilfenangelegenheiten von Schülerinnen und Schülern Zuständigen sollen auch als Verantwortliche im Sinne der DSGVO gelten.

Zu Art. 56 Z 5, 6 und 7 (§ 15 Abs. 6, 7 und 8; Entfall des § 15 Abs. 5, 9 und 10):

Die bisher in Abs. 6 genannten Daten sollen in die neu eingefügte Anlage aufgenommen werden.

In Abs. 7 erfolgen Anpassungen der übermittelnden Einrichtungen und soll festgelegt werden, unter Angabe welcher Daten eine Anfrage durch die Schülerbeihilfenbehörden zu erfolgen hat. Weiters wird im neuen Abs. 8 eine Löschungsfrist für zum Zweck der Gewährung von Schülerbeihilfen verarbeitete Daten vorgesehen, die mit Ablauf des 31. Juli des der letzten Antragstellung siebtfolgenden Kalenderjahres festgelegt werden soll. Die Frist ist so gewählt, dass für einen späteren Beihilfenanspruch relevante Daten jedenfalls nicht neu zu erfassen sein sollen.

Abs. 9 hat zu entfallen, da die bisher durch Verordnung zu regelnde Beschreibung der Daten direkt in das Gesetz (Anlage) übernommen werden soll.

Zu Art. 56 Z 8 (§ 25):

Hier erfolgt die Neufassung der Vollzugsbestimmung aufgrund der geänderten Ressortzuständigkeiten.

Zu Art. 56 Z 9 (§ 26 Abs. 20):

Diese Bestimmung regelt das In- und Außerkrafttreten, das hinsichtlich der datenschutzrechtlich relevanten Änderungen in Übereinstimmung mit dem Wirksamwerden der DSGVO mit 25. Mai 2018, hinsichtlich der geänderten Ressortbezeichnungen und sonstigen rein redaktionellen Änderungen mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt vorgesehen ist.

Das Inkrafttreten des § 13 Z 1 in der Fassung des Bildungsreformgesetzes 2017 soll in Übereinstimmung mit dem dort festgelegten Zeitpunkt erst mit 1. Jänner 2019 erfolgen.

Zu Art. 56 Z 10 (Anlage):

In der Anlage zu § 15 Abs. 6 sind die bisher in Abs. 6 genannten Daten, zu deren Verarbeitung die Beihilfenbehörden berechtigt sind, angeführt.

Der Anlage umfasst infolge des Entfalls der Verordnungsermächtigung in § 15 Abs. 9 weiters die Verarbeitung der personenbezogenen Daten in Form ihrer Übermittlung durch die in § 15 Abs. 7 genannten Einrichtungen an die Schülerbeihilfenbehörden. Die Anlage enthält diesbezüglich die Beschreibung der Durchführung des automationsunterstützten Datenverkehrs im Detail, wie sie bereits mit der Verordnung der Bundesministerin für Bildung über die Durchführung des automationsunterstützten Datenverkehrs in Verfahren vor den Schülerbeihilfenbehörden (Schülerbeihilfen-ADV-Verordnung), BGBl. II Nr. 286/2017, kundgemacht wurde. Bei den personenbezogenen Daten, die von der automationsunterstützten Übermittlung betroffen sind, handelt es sich um Einkommensdaten, Personendaten sowie Daten über den Schulbesuch des Beihilfenwerbers oder der Beihilfenwerberin.

Zum 5. Hauptstück (Digitales, Wirtschaft)

Besonderer Teil

Zum 5. Hauptstück (Digitales und Wirtschaft)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung der Bundesgesetze dieses Hauptstücks gründet sich auf Art. 10 Abs. 1 Z 4 B-VG („Bundesfinanzen und Monopolwesen“); Art. 10 Abs. 1 Z 6 B-VG („Zivilrechtswesen“), Art. 10 Abs. 1 Z 8 B-VG (Angelegenheiten des Gewerbes und der Industrie, Bekämpfung des unlauteren Wettbewerbes, Kartellrecht,…), Art. 10 Abs. 1 Z 16 B-VG („Einrichtung der Bundesbehörden…“); auf die Bedarfsgesetzgebungskompetenz für das Verwaltungsverfahren nach Art. 11 Abs. 2 B-VG; auf „Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr“ gemäß § 2 DSG.

Zu Art. 57 (Änderung des E-Government-Gesetzes)

Zu Art. 57 Z 1 bis 16, 18 bis 25 (Einträge im Inhaltsverzeichnis zu den §§ 8, 14, 15 bis 18 und 22, § 3, § 4 Abs. 1, 2, 4, 5 und 6, § 4a Abs. 3 bis 5, § 4b, § 5 Abs. 1 bis 3, § 6 Abs. 2, 4 und 5, § 7 Abs. 2, § 8 samt Überschrift, § 9 Abs. 2, § 10 Abs. 1 und 2, § 11, § 12, § 13, § 14 samt Überschrift, § 14a

Abs. 2, die Überschrift zu § 15, § 15 Abs. 1, die Überschrift zu § 16, § 16 Abs. 2, § 17 samt Überschrift, die Überschrift zu § 18, § 18 Abs. 1 und 2, § 19 Abs. 2 und 3, die Überschrift zu § 22, § 22 Abs. 1, § 24 Abs. 3, § 25 Abs. 2):

Anstelle der Bestimmungen des DSG 2000 sollen nun die kohärenten Bestimmungen der Datenschutz-Grundverordnung (DSGVO) zitiert werden. Ebenso sollen die bisherigen Begriffe des DSG 2000 daher durch die Begriffe der DSGVO ersetzt werden. Es sind daher die Begriffe „Datenanwendung" in „Datenverarbeitung", „Verwendung" in „Verarbeitung", „verwenden" in „verarbeiten", „Zustimmung" in „Einwilligung", „Auftraggeber" in „Verantwortlicher", „Dienstleister" in „Auftragsverarbeiter" sowie in den anwendbaren Fällen „Daten" in „personenbezogene Daten" zu ändern.

Der Vollständigkeit halber ist darauf hinzuweisen, dass die Änderungen der Novelle BGBl. I Nr. 121/2017 zwar mit 1. August 2017 in Kraft getreten sind, jedoch großteils erst Anwendung finden, wenn die technischen und organisatorischen Voraussetzungen für den Echtbetrieb des E-ID vorliegen. Dieser Zeitpunkt ist vom Bundesminister für Inneres im Bundesgesetzblatt kundzumachen (vgl. § 24 Abs. 6 letzter Satz). Gemäß § 25 Abs. 3 ist für bis zum Zeitpunkt der Aufnahme des Echtbetriebes ausgestellte Bürgerkarten die Rechtslage vor Inkrafttreten dieses Bundesgesetzes, BGBl. I Nr. 121/2017, anzuwenden. Eine Novellierung dieser zwar noch anzuwendenden, aber außer Kraft getretenen Rechtsvorschriften im Hinblick auf die datenschutzrechtlichen Begriffe (vgl. erster Absatz) ist nicht möglich. Bei der Anwendung der alten Rechtslage sind diese daher im Sinne der jeweiligen korrespondierenden Begriffe nach der DSGVO und des DSG zu verstehen.

Zu Art. 57 Z 17 (§ 9 Abs. 1):

In § 9 Abs. 1 soll sich die Zurechnung einer Datenverarbeitung zu einem bestimmten staatlichen Tätigkeitsbereich nun nicht mehr aus ihrer Registrierung im (aufgrund des DSG weggefallenden) Datenverarbeitungsregister bzw. aus der (aufzuhebenden) Standard- und Musterverordnung ergeben, sondern durch die Registrierung bei der Stammzahlenregisterbehörde.

Zu Art. 58 (Änderung des Signatur- und Vertrauensdienstegesetzes)

Zu Art. 58 Z 1 (§ 10 Abs. 2):

Eine direkte Bezugnahme auf eine Bestimmung der DSGVO anstelle der Bestimmung des DSG 2000 ist nicht möglich, da die DSGVO unmittelbar gilt und daher nicht als Voraussetzung für eine Datenübermittlung im nationalen Recht verankert werden soll. Die vom VDA vorzunehmende Interessenabwägung hat jedenfalls auch im Einklang mit der DSGVO zu erfolgen.

Zu Art. 59 (Änderung des Unternehmensserviceportalgesetzes)

Zu Art. 59 Z 1 bis 3 (Überschrift zu § 4, § 4 Abs. 1 erster Satz und zweiter Satz):

Anstelle des DSG 2000 sollen nun die Datenschutz-Grundverordnung (DSGVO) zitiert sowie der Begriff „Dienstleisterstellung" durch den Begriff „Auftragsverarbeiterstellung" ersetzt werden.

Zu Art. 60 (Änderung des Dienstleistungsgesetzes)

Zu Art. 60 Z 1 und 2 (§ 6 Abs. 6, § 15 Abs. 6):

Es handelt sich um redaktionelle Anpassungen an die Datenschutz-Grundverordnung.

Zu Art. 61 (Änderung des Informationsweiterverwendungsgesetzes)

Zu Art. 61 Z 1 (§ 2 Abs. 3):

Es handelt sich um redaktionelle Anpassungen an die Datenschutz-Grundverordnung.

Zu Art. 62 (Änderung des Wettbewerbsgesetzes)

Zu Art. 62 Z 1 (§ 10 Abs. 1 und 1a):

Die in § 10 Absatz 1 vorgenommenen Änderungen dienen der redaktionellen Anpassung an das Datenschutzgesetz idF BGBl. I Nr. 120/2017.

Die Eingliederung des § 14 Abs. 3 in § 10 als neuer Abs. 1a dient der Klarstellung sowie der Absicherung der notwendigen Datenübermittlung von Kriminalpolizei, Staatsanwaltschaft und Gerichten an die BWB. § 10 Abs. 1a gilt als ausdrückliche gesetzliche Ermächtigung iSd § 76 Abs. 4 StPO. Im Übrigen sind die Voraussetzungen von § 76 Abs. 4 StPO und Art. 10 DSGVO zu beachten.

§10 Abs. 1a gilt außerdem als ausdrückliche gesetzliche Grundlage iSd § 37a JN.

Zu Art. 62 Z 2 (§ 11 Abs. 3 bis 5):

Sofern in § 11 Abs. 3 bis 6 auf die Ziele der BWB Bezug genommen wurde, sind jene gemeint, die in § 1 Abs. 1 WettbG aufgezählt sind. Bei den genannten Aufgaben handelt es sich um jene, die in § 2 Abs. 1 WettbG aufgelistet sind.

Abs. 3 des Entwurfs ermächtigt die BWB im Rahmen ihres gesetzlichen Auftrages, sämtliche personenbezogene Daten zu verarbeiten, die zur Erreichung ihrer Ziele und zur Erfüllung ihrer Aufgaben erforderlich sind. Zu betonen ist in diesem Zusammenhang, dass es sich dabei nicht um Daten handelt, die Art. 9 DSGVO (besonderen Kategorien von personenbezogenen Daten) sind.

Sofern keine allgemeinen Regeln über die Aufbewahrungsdauer von Verwaltungsakten bestehen oder sich eine Pflicht zur Aufbewahrung aus anderen gesetzlichen Vorschriften ergibt, ist hinsichtlich der Aufbewahrung personenbezogener Daten Art. 5 Abs. 1 lit. e DSGVO anzuwenden. Hinsichtlich bestimmter Verfahren ist es unumgänglich, die Möglichkeit einer langfristigen Aufbewahrung von Akten samt der darin allenfalls enthaltenen personenbezogenen Daten sicherzustellen. Dies betrifft einerseits die bei der BWB anzumeldenden Unternehmenszusammenschlüsse (3. Abschnitt KartG iVm § 10a WettbG), da es hier auch noch nach Jahren möglich sein muss, die anmeldungskonforme Durchführung des Zusammenschlusses zu prüfen, andererseits insbesondere Verfahren über Wettbewerbsrechtsverletzungen. Daten aus den letztgenannten Verfahren müssen aufbewahrt werden dürfen, solange sie aufgrund offener Verjährungsfristen als Beweismittel im Rahmen eines Schadenersatzverfahrens in Frage kommen. Die RL 2014/104/EU hat Geschädigten diesbezüglich unter bestimmten Voraussetzungen Anspruch auf Offenlegung von Beweismitteln aus Akten der Wettbewerbsbehörden eingeräumt (vgl. §§ 37a ff KartG 2005). Eine vorzeitige Löschung von Daten aus solchen Verfahren würde dem Zweck der genannten Richtlinie diametral zuwiderlaufen.

Abs. 4 des Entwurfs sieht eine notwendige Einschränkung des in Artikel 15 DSGVO vorgesehenen Auskunftsrechts vor. Aufgrund des übergeordneten öffentlichen Interesses an der Aufrechterhaltung der Wettbewerbsordnung (lit. e) und der damit verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (lit. h) wird von der Öffnungsklausel des Artikel 23 DSGVO Gebrauch gemacht. Eine Kernaufgabe der BWB ist die Aufdeckung und Ermittlung von Verstößen gegen Kartellrecht. Aus offenkundigen Gründen würde es dem im überwiegenden öffentlichen Interesse gelegenen Zweck diesbezüglicher Ermittlungen zuwiderlaufen, könnte über das Instrument des Auskunftsrechts Kenntnis über den Stand laufender Ermittlungen erlangt werden.

Ähnliches gilt für die in Abs. 5 des Entwurfs festgelegte Beschränkung des Widerspruchsrechts gemäß Artikel 21 DSGVO. Dieses würde im Großteil der Verwaltungsbereiche einen geordneten Vollzug verunmöglichen. Auch hier wird daher von der Möglichkeit des Artikel 23 Absatz 1 DSGVO Gebrauch gemacht, dieses in genereller Weise eingeräumte Widerspruchsrecht mit Blick auf das übergeordnete öffentliche Interesse an der Aufrechterhaltung der Wettbewerbsordnung (lit. e) und die damit verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (lit. h) zu beschränken.

Zu Art. 62 Z 3 (§ 14 Abs. 3):

Der Entfall des § 14 Abs. 3 ergibt sich aus Z 1.

Zu Art. 63 (Änderung der Gewerbeordnung)

Zu Art. 63 Z 1 (§ 77a Abs. 7 GewO 1994):

Die vorgeschlagene Änderung soll der Verbesserung des Datenflusses an die Europäische Kommission dienen; konkret soll die Erfüllung der Berichtspflichten Österreichs an die Europäische Kommission sichergestellt werden – siehe den Durchführungsbeschluss 2012/795/EU vom 12. Dezember 2012 zur Festlegung, welche Art von Informationen die Mitgliedstaaten in welcher Form und mit welcher Häufigkeit für die Berichterstattung über die Umsetzung der Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates über Industrieemissionen zu übermitteln haben, ABl. Nr. L 349 vom 19.12.2012 S. 57.

Zu Art. 63 Z 2 (§ 151 GewO 1994):

Die vorgeschlagenen Änderungen dienen vor allem der terminologischen Anpassungen an die DSGVO. Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der in § 151 Gewerbeordnung 1994 verwendeten Begriffe erforderlich scheint, sollen diese an die Definitionen der DSGVO angeglichen werden. Beispielsweise sollen die Begriffe „Betroffene“ durch „betroffene Person, „Datei“ („Kunden- und Interessentendatei“) durch „Dateisystem“ im Sinne des Art. 4 Z 6 DSGVO und „Auftraggeber“ (§ 4 Z 5 DSG 2000) durch „Verantwortlicher“ im Sinne des Art. 4 Z 7 DSGVO ersetzt werden.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO entspricht dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Überdies soll im Sinne der neuen datenschutzrechtlichen Terminologie klargestellt werden, dass es sich bei den von Adressverlagen verarbeiteten Daten um personenbezogene Daten handelt.

Zudem soll im Hinblick auf die neuen Begrifflichkeiten die Wortfolge „sensible Daten“ auf „besondere Kategorie personenbezogener Daten“ (vgl. Art. 9 DSGVO) angepasst werden.

Zu Abs. 1:

Es handelt sich um Verweisanpassungen an die neuen datenschutzrechtlichen Regelungen der DSGVO und des DSG.

Zu Abs. 1 bis 6 und 9 bis 10:

Es handelt sich im Wesentlichen um terminologische Anpassungen sowie um Verweisanpassungen an die DSGVO. Inhaltliche Änderungen sind damit nicht verbunden.

Zu Abs. 7:

Da sich das Auskunftsrecht der betroffenen Person künftig direkt aus Art. 15 DSGVO ergibt, hat eine Verweisanpassung zu erfolgen.

Zu Abs. 8:

Aufgrund der Fristverkürzung in Art. 12 Abs. 3 DSGVO von acht Wochen auf einen Monat ist eine Anpassung erforderlich. Die Frist von einem Monat kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

Zu Abs. 11:

Im Hinblick auf das unionsrechtliche Transformationsverbot ist eine Wiederholung des Widerspruchrechtes gegen Verarbeitungen zum Zweck der Direktwerbung in einer nationalen Vorschrift nicht zulässig, weshalb Satz 1 zu entfallen hat und Satz 2 entsprechend durch einen vorangestellten Verweis ergänzt wird.

Zu Art. 63 Z 3 (§ 352b GewO 1994):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird der Begriff „Daten“ um das Wort „personenbezogenen“ erweitert. Weiters wird gemäß der Begriffsbestimmung des Art. 4 Z 2 DSGVO der Begriff „Verwendung“ durch den Begriff „Verarbeitung“ ersetzt.

Zu Art. 63 Z 4 (§ 365m1 Abs. 10 Z 4 GewO 1994):

Es handelt sich um eine Verweisanpassung an die neuen datenschutzrechtlichen Regelungen der DSGVO und des DSG.

Zu Art. 63 Z 5 (§ 373a Abs. 5 GewO 1994):

Es hat sich herausgestellt, dass die im Dienstleisterregister eingetragenen Personen verwechselt werden können, da die gemäß dem geltenden § 373a Abs. 5 GewO 1994 erfassten Informationen nicht gewährleisten, dass mehrfach vorkommende Namen sicher unterschieden werden können.

Personen, die sich im Dienstleisterregister registrieren lassen, sollen sich jedoch darauf verlassen können, dass jene Rechte, die sie dort registrieren lassen, ihnen auch eindeutig zugeordnet werden können. Die im Dienstleisterregister erfassten Informationen sollen daher um das Geburtsdatum und die Staatsangehörigkeit ergänzt werden, damit den im Dienstleisterregister geführten Personen eine ausreichend verlässliche Datenquelle zur Verfügung steht.

Zu Art. 64 (Änderung des Berufsausbildungsgesetzes)

Allgemeines:

Allgemein wurde in den novellierten Bestimmungen die Bezeichnung des Bundesministeriums für Wissenschaft, Forschung und Wirtschaft gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, jeweils in Bundesministerium für Digitalisierung und Wirtschaftsstandort umbenannt.

Zu Art. 64 Z 1 (§ 19c Abs. 7 BAG):

§ 19 c Abs. 7 erster Satz BAG ermöglicht es den Wirtschaftskammern, sich zur Vorbereitung und Durchführung der Entscheidungen der Lehrlingsstellen hinsichtlich der Beihilfen für die betriebliche Ausbildung von Lehrlingen einer eigenen Gesellschaft oder sonstiger geeigneter Einrichtungen als Dienstleister zu bedienen. Dies betrifft einerseits die Abwicklung der Beihilfen im eigentlichen Sinn,

wofür der Begriff „Dienstleister“ nach wie vor zutreffend und auch legistisch/sprachlich zulässig ist. Sofern aber in diesem Zusammenhang die – durch die betreffende Gesellschaft oder Einrichtung – durchgeführten Tätigkeiten auf dem Gebiet der Datenverarbeitung angesprochen sind, ist dafür gemäß Art. 4 Z 8 DSGVO nunmehr der Begriff „Auftragsverarbeiter“ zu verwenden. Um daher in Hinkunft für beide Tätigkeitsbereiche die rechtlich korrekten und auch sprachlich adäquaten Bezeichnungen zu verwenden, sollen die Begriffe „Dienstleister“ und „Auftragsverarbeiter“ kumulativ angeführt werden.

Zu Art. 64 Z 2 (§ 19e Abs. 1 BAG):

Gemäß § 19e Abs. 1 BAG hat der Bundesminister für Wirtschaft, Familie und Jugend (nunmehr Bundesministerin für Digitalisierung und Wirtschaftsstandort) die Zweckmäßigkeit und Wirkung der vom Förderausschuss gemäß § 19c festgelegten Beihilfen zu prüfen, wobei er sich dabei erforderlichenfalls geeigneter externer Einrichtungen als Dienstleister bedienen kann. Hier gelten die Ausführungen wie oben zu Ziffer 1 analog: sofern bei der Prüfung der Zweckmäßigkeit und Wirkung von Beihilfen die Datenverarbeitung angesprochen ist, firmiert gemäß Art. 4 Z 8 DSGVO eine herangezogene Einrichtung für diese Tätigkeit nunmehr unter dem Begriff „Auftragsverarbeiter“. Daher werden auch hier die Begriffe „Dienstleister“ und „Auftragsverarbeiter“ kumulativ angeführt.

Zu Art. 64 3 (§ 19f BAG):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird der Begriff „Daten“ jeweils um das Wort „personenbezogene“ erweitert.

Zu Art. 64 Z 4 (§ 19g Abs. 1 BAG):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird der Begriff „Daten“ um das Wort „personenbezogener“ erweitert bzw. statt des Begriffes „Datenarten“ nun der Begriff „Arten von personenbezogenen Daten“ verwendet.

Zu Art. 64 Z 5 (§ 19g Abs. 1):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird nunmehr der Begriff „Daten“ jeweils um das Wort „personenbezogene“ erweitert.

Zu Art. 64 Z 6 und 7 (§ 19g Abs. 2 und 3):

Einerseits wird entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO nunmehr der Begriff „Daten“ jeweils um das Wort „personenbezogene“ erweitert. Gemäß der Begriffsbestimmung des Art. 4 Z 8 DSGVO wird der Begriff „beauftragte Dienstleister“ durch den Begriff „Auftragsverarbeiter“ ersetzt. Weiters wird der Begriff „überlassen“ durch „übermitteln“ ersetzt.

Zu Art. 64 Z 8 und 9 (§ 20 Abs. 7 und § 31d Abs. 5):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird der Begriff „Daten“ um den Begriff „personenbezogenen“ bzw. „personenbezogene“ erweitert.

Zu Art. 65 (Änderung des Ingenieurgesetzes 2017)

Zu Art. 65 Z 1 (§ 11):

Entsprechend der Begriffsbestimmung des Art. 4 Z 1 DSGVO wird der Begriff „Daten“ um das Wort „personenbezogenen“ erweitert. Weiters wird gemäß der Begriffsbestimmung des Art. 4 Z 2 DSGVO der Begriff “Verwendung“ durch den Begriff „Verarbeitung“ ersetzt.

Die Bezeichnungen der betreffenden Bundesministerien wurden gemäß der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, angepasst.

Zu Art. 66 (Änderung des Bilanzbuchhaltungsgesetzes 2014)

Zu Art. 66 Z 1 (§ 52a Abs. 14):

Auf Grund der in der DSGVO ohnehin enthaltenen und unmittelbar anzuwendenden Bestimmungen kann diese Bestimmung entfallen.

Zu Art. 66 Z 2 (§ 52e Abs. 4):

§ 52e Abs. 4 erster Satz kann ersatzlos entfallen, da die Meldepflichten gemäß § 17 Abs. 1 des Datenschutzgesetzes 2000 ebenfalls entfallen sind. § 53e Abs. 4 zweiter Satz kann ebenfalls entfallen; die Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 1 DSGVO vom Verantwortlichen durchzuführen; dies ist in diesem Fall die Bilanzbuchhaltungsbehörde.

Zu Art. 66 Z 3 (§ 67c):

Mit Geltungsbeginn der DSGVO sollen auch die Änderungen des Bilanzbuchhaltungsgesetzes 2014 in Kraft treten.

Zu Art. 67 (Änderung des Wirtschaftskammergesetzes 1998)

Zu Art. 67 Z 1 (§ 72 Abs. 1):

Es werden lediglich die Verweise angepasst.

Zu Art. 67 Z 2 (§ 72 Abs. 3):

§ 72 Abs. 3 ist obsolet geworden und kann ersatzlos entfallen.

Zu Art. 67 Z 3 und 4 (§ 72 Abs. 6 und § 74 Abs. 2):

Es werden lediglich die Verweise angepasst.

Zu Art. 67 Z 5 (§ 150 Abs. 7):

Mit Geltungsbeginn der DSGVO sollen auch die Änderungen des Wirtschaftskammergesetzes 1998 in Kraft treten.

Zu Art. 68 (Änderung des Wirtschaftstreuhandberufsgesetzes 2017)

Zu Art. 68 Z 1 (Inhaltsverzeichnis):

Durch die Anfügung eines § 238 Abs. 2 wird eine Änderung der Paragraphenüberschrift und damit auch des Inhaltsverzeichnisses erforderlich.

Zu Art. 68 Z 2 (96 Abs. 15):

Auf Grund der in der DSGVO ohnehin enthaltenen und unmittelbar anzuwendenden Bestimmungen kann diese Bestimmung entfallen.

Zu Art. 68 Z 3 (§ 100 Abs. 4):

§ 100 Abs. 4 erster Satz kann ersatzlos entfallen, da die Meldepflichten gemäß § 17 Abs. 1 des Datenschutzgesetzes 2000 ebenfalls entfallen sind. § 100 Abs. 4 zweiter Satz kann ebenfalls entfallen; die Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 1 DSGVO vom Verantwortlichen durchzuführen; dies ist in diesem Fall die Kammer der Wirtschaftstreuhänder.

Zu Art. 68 Z 4 (§ 183):

Es werden lediglich die Verweise angepasst und eine sprachliche Bereinigung vorgenommen.

Zu Art. 68 Z 5 (§ 238a):

Mit Geltungsbeginn der DSGVO sollen auch die Änderungen des Wirtschaftstreuhandberufsgesetzes 2017 in Kraft treten.

Zu Art. 69 (Änderung des Ziviltechnikerkammergesetzes 1993)

Zu Art. 69 Z 1 (§ 18 Abs. 2 Z 7):

Es werden lediglich die Verweise angepasst.

Zu Art. 69 Z 2 (§ 34 Abs. 3):

Der neue Abs. 3 ermächtigt die Architekten- und Ingenieurkonsulentenkammern personenbezogene Daten ihrer Mitglieder, Anwärter, Funktionäre usw. im Rahmen ihrer gesetzlichen Aufgaben zu verarbeiten. Verantwortliche im Sinne der DSGVO sind die Architekten- und Ingenieurkonsulentenkammern**.**

Zum 6. Hauptstück (Finanzen)

Allgemeines

Zu Art. 70 und 71 (Änderung der Bundesabgabenordnung und der Abgabenexekutionsordnung):

Die Datenschutz-Grundverordnung wird zwar unmittelbar wirksam, bedarf aber trotzdem in einigen Bereichen einer Durchführung im innerstaatlichen Recht. Darüber hinaus enthält sie Regelungsspielräume („Öffnungsklauseln“) für den nationalen Gesetzgeber. Während die notwendige Durchführung bzw. Umsetzung der unionsrechtlichen Vorgaben hinsichtlich allgemeiner Angelegenheiten des Schutzes

personenbezogener Daten durch das Datenschutz-Anpassungsgesetz 2018 (BGBl. I Nr. 120/2017) im Datenschutzgesetz (DSG) erfolgte, fällt der überwiegende Teil der Öffnungsklauseln nicht in den Bereich der allgemeinen Angelegenheiten des Datenschutzes und wurde deshalb nicht im DSG ausgeübt. Dementsprechend ist es erforderlich, durch Ausüben der Regelungsspielräume der DSGVO (zB Art. 23 DSGVO) spezifische datenschutzrechtliche Regelungen für das Abgabenverfahren zu schaffen.

Die Verarbeitung personenbezogener Daten bei Wahrnehmung einer im öffentlichen Interesse gelegenen Aufgabe oder in Ausübung öffentlicher Gewalt ist gemäß Art. 6 Abs. 1 lit. e in Verbindung mit Abs. 3 DSGVO nur bei Vorliegen einer entsprechenden Rechtsgrundlage zulässig. Es soll daher eine (allgemeine) Rechtsgrundlage für das Abgabenverfahren geschaffen werden, die eine Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im Abgabenverfahren sicherstellt.

Einen weiteren Schwerpunkt stellt die Nutzung der Regelungsspielräume der DSGVO dar. Insbesondere die Öffnungsklausel des Art. 23 DSGVO ermöglicht dem nationalen Gesetzgeber bestimmte Rechte der betroffenen Person und Pflichten des Verantwortlichen zu beschränken. Die Beschränkung muss den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine notwendige und verhältnismäßige Maßnahme darstellen. Als legitimes Beschränkungsziel im Sinne des Art. 23 Abs. 1 lit. e DSGVO ist der Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses etwa im Haushalts- und Steuerbereich besonders hervorzuheben.

Zusammenfassend ist ein wesentliches Ziel der Novellierung, die aus Sicht der Behörde und der Bürger bewährte Verwaltungspraxis im Bereich der Abgabenverfahren beizubehalten. Diese hat auch bereits bisher ein hohes Maß an Datenschutz (zB abgabenrechtliche Geheimhaltungspflicht gemäß § 48a BAO) geboten, und soll damit weiterhin eine funktionierende Abgabenerhebung gewährleisten.

Überdies erfolgen eine Begriffsanpassung sowie eine Anpassung der nicht mehr aktuellen Verweise.

Die Änderungen sollen mit 25. Mai 2018 in Kraft treten.

Zu Art. 72 (Änderung des Finanzstrafgesetzes):

Die Richtlinie (EU) 2016/680, ABl. Nr. L 119 vom 4.5.2016 S. 89, zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden Datenschutz-RL) bedarf der Umsetzung ins innerstaatliche Recht. Bisher gab das Recht der Europäischen Union im Bereich des Strafrechts nur für die polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten datenschutzrechtliche Bestimmungen vor (Rahmenbeschluss 2008/977/JI des Rates, ABl. Nr. L 350 vom 27.11.2008 S. 60). Die Umsetzung der Datenschutz-RL, welche über diesen Rahmenbeschluss hinausgeht und jegliche Datenverarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung umfasst, soll für den Bereich des Finanzstrafrechts im Finanzstrafgesetz erfolgen, um Kohärenz und Rechtssicherheit im Verhältnis zu den finanzstraf- und abgabenrechtlichen Bestimmungen zu gewährleisten. Dabei soll, soweit sachdienlich, auf die Bestimmungen des Datenschutzgesetzes verwiesen werden.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich hinsichtlich dieses Hauptstücks aus Art. 10 Abs. 1 Z 1 und Z 4 B-VG (Bundesfinanzen und Monopolwesen) und aus § 7 Abs. 6 F-VG 1948 sowie aus Art. 10 Abs. 1 Z 6 B-VG (Strafrechtswesen).

Zu Art. 70 Änderung der Bundesabgabenordnung)

Zu Art. 70 Z 1 (§ 48b BAO):

Die Änderung dient der Anpassung der Begriffsverwendung und des Verweises an die DSGVO. Deren Begriffsdefinition tritt nun an die Stelle der Begriffsdefinition im DSG 2000.

Zu Art. 70 Z 2 (§ 48d bis 48i BAO):

Zu § 48d BAO:

Zu Abs. 1: Die Verarbeitung personenbezogener Daten bei Wahrnehmung einer im öffentlichen Interesse gelegenen Aufgabe oder in Ausübung öffentlicher Gewalt ist gemäß Art. 6 Abs. 1 lit. e in Verbindung mit Abs. 3 DSGVO nur bei Vorliegen einer entsprechenden Rechtsgrundlage zulässig. Neben den spezifischen gesetzlichen Grundlagen der einzelnen Abgabenvorschriften bildet § 48d Abs. 1 die (generelle) Rechtsgrundlage dafür, dass Abgabenbehörden personenbezogene Daten verarbeiten dürfen. In dieser Funktion tritt er an die Stelle des bisher geltenden § 114 Abs. 4. Auch eine Verarbeitung von

personenbezogenen Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten ursprünglich erhoben wurden (Weiterverarbeitung), kann – sofern dafür nicht ohnehin eine spezifische Rechtsgrundlage besteht – auf Grundlage des § 48d Abs. 1 erfolgen.

Die Bestimmung gilt auch für nicht automationsunterstützt verarbeitete Daten, für die ebenfalls die DSGVO bzw. das DSG anwendbar sein kann (vgl. Art. 2 Abs. 1 DSGVO, § 4 Abs. 5 DSG).

Die Bestimmung gilt gemäß § 2a und § 269 Abs. 1 auch für Verwaltungsgerichte sowie im Rahmen des § 2 lit. b auch in Monopolverfahren. Sie gilt nicht nur für die Abgabenerhebung, sondern ist zB auch auf die Auszahlung von Beihilfen wie etwa der Familienbeihilfe anzuwenden.

Zu Abs. 2: Art. 9 DSGVO lässt die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter bestimmten Voraussetzungen zu.

Unter den Begriff „besondere Kategorien personenbezogener Daten“ fallen unter anderem

- personenbezogene Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- personenbezogene Daten, aus denen die religiöse oder weltanschauliche Überzeugung hervorgeht,
- Gesundheitsdaten.

Art. 9 Abs. 2 lit. g DSGVO erlaubt die Verarbeitung, wenn eine gesetzliche Grundlage besteht und die Datenverarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. § 48d Abs. 2 kommt diesen Erfordernissen (gemeinsam mit den jeweiligen Vorschriften der Materiengesetze bzw. – bei deren Fehlen – mit Abs. 1) für bestimmte Datenverarbeitungen nach, die einerseits eine hohe Sensibilität aufweisen, andererseits in einem „erheblichen öffentlichen Interesse“ im Sinn des Art. 9 Abs. 2 lit. g DSGVO liegen. Mit § 48d Abs. 2 wird damit für die angesprochenen Bereiche die Rechtmäßigkeit der Verarbeitung abgesichert. Das gilt insbesondere für die abgabenrechtliche Berücksichtigung der

1. Beiträge für die freiwillige Mitgliedschaft bei Berufsverbänden,
2. verpflichtenden Beiträge an Kirchen und Religionsgesellschaften,
3. freigebigen Zuwendungen (Spenden),
4. Kosten einer Krankheit oder Behinderung.

Die abgabenrechtliche Berücksichtigung dieser Aufwendungen ist zur rechtsrichtigen und gleichmäßigen Besteuerung zwingend erforderlich, womit ein „erhebliches öffentliches Interesse“ im Sinn des Art. 9 Abs. 2 lit. g DSGVO unzweifelhaft gegeben ist.

Der erste Punkt betrifft die Gewerkschaftszugehörigkeit. Die Wahrung des Grundrechts auf Datenschutz wird hier insbesondere durch die abgabenrechtliche Geheimhaltungspflicht gemäß § 48a garantiert, wenn die Gewerkschaftszugehörigkeit gegenüber der Abgabenbehörde im Zuge des Veranlagungsverfahrens offenbart wird. Wird die Gewerkschaftszugehörigkeit dem Dienstgeber zum Zwecke der Berücksichtigung bei der Lohnsteuerberechnung gemäß § 62 Z 3 EStG 1988 offenbart, unterliegt dieser den einschlägigen arbeitsrechtlichen Verpflichtungen.

Der zweite Punkt betrifft die religiöse oder weltanschauliche Überzeugung. Der dritte Punkt kann mehrere besondere Kategorien personenbezogener Daten betreffen: Es kann in bestimmten Fällen möglich sein, aus dem Spendenempfänger auf eine politische Meinung, eine religiöse oder weltanschauliche Überzeugung, unter Umständen sogar auf dessen Gesundheitszustand zu schließen. Die Erlaubnis der Verarbeitung personenbezogener Daten ist in diesen Fällen erforderlich, um die steuerliche Abzugsfähigkeit der Beiträge an eine Gewerkschaft bzw. an eine Kirche oder Religionsgesellschaft sowie von Spenden zu ermöglichen. Die Wahrung des Grundrechts auf Datenschutz wird für die Punkte 2 und 3 insbesondere garantiert durch

- die gemäß § 12 der Sonderausgaben-Datenübermittlungsverordnung, BGBl. II Nr. 289/2016, verpflichtende Verwendung eines verschlüsselten bereichsspezifischen Personenkennzeichens (vbPK) gemäß § 13 Abs. 2 des E-Government-Gesetzes, BGBl. I Nr. 10/2004,
- § 14 der Sonderausgaben-Datenübermittlungsverordnung,
- die abgabenrechtliche Geheimhaltungspflicht gemäß § 48a.

Zusätzlich ist zu berücksichtigen, dass die unter Punkt eins bis vier angeführten Bestimmungen begünstigend sind und keine Verpflichtung des Abgabepflichtigen zur Bekanntgabe der Daten besteht.

Die Regelung einer Ausnahme von Art. 9 Abs. 1 DSGVO steht in einem angemessenen Verhältnis zum Zweck der materiellrechtlich einschlägigen Bestimmungen, die die steuerliche Abzugsfähigkeit von Zahlungen an bestimmte Organisationen erlauben. Das gilt vor allem angesichts der besonderen

datenschutzrechtlichen Vorkehrungen, wie etwa der Verwendung von verschlüsselten bereichsspezifischen Personenkennzeichen.

Der vierte Punkt betrifft Gesundheitsdaten. Die Ertragsteuer ist vom Leistungsfähigkeitsprinzip geprägt. Ein Aspekt des Leistungsfähigkeitsprinzips wird „subjektives Nettoprinzip“ genannt. Dieses Prinzip gebietet die steuerliche Berücksichtigung der Tatsache, dass Einkommensteile zur Deckung besonderer persönlicher Ausgabenerfordernisse – etwa im Fall einer Krankheit oder Behinderung – benötigt werden. Es wird unter anderem durch die Abzugsfähigkeit von außergewöhnlichen Belastungen (§ 34 und § 35 EStG 1988) verwirklicht.

Die Regelung des Abs. 2 steht in einem angemessenen Verhältnis zum Zweck, durch die steuerliche Absetzbarkeit von Krankheits- und Behinderungskosten die Verfassungsmäßigkeit der Steuererhebung sicherzustellen.

Die Wahrung des Grundrechts auf Datenschutz wird insbesondere garantiert durch

- das Erfordernis der Einwilligung der betroffenen Person in die elektronische Datenübermittlung gemäß § 35 Abs. 8 erster Satz EStG 1988.
- die Zweckbindung und Löschungsbestimmung des § 35 Abs. 8 vorletzter und letzter Satz EStG 1988,
- die teilweise Möglichkeit, Pauschbeträge anstelle von tatsächlichen Kosten absetzen zu können,
- das Unterlassen der Speicherung der erforderlichen personenbezogenen Daten, die durch das Bundesamt für Soziales und Behindertenwesen, erhoben wurden, seitens des BMF,
- die abgabenrechtliche Geheimhaltungspflicht gemäß § 48a.

Exkurs (zu §§ 48e bis 48g BAO):

Soweit eine Abgabenbehörde oder ein Verwaltungsgericht jeweils allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist die Abgabenbehörde oder das Verwaltungsgericht als datenschutzrechtlicher Verantwortlicher im Sinn des Art. 4 Z 7 DSGVO anzusehen. Infolge dessen treffen die Pflichten des datenschutzrechtlich Verantwortlichen im Anwendungsbereich der BAO entweder eine Abgabenbehörde oder ein Verwaltungsgericht. Die §§ 48e bis 48g schränken die datenschutzrechtlichen Rechte gegenüber dem Verantwortlichen und die Pflichten des Verantwortlichen ein.

Zu § 48e BAO:

Werden personenbezogene Daten bei der betroffenen Person erhoben, besteht gemäß Art. 13 Abs. 1 und 2 DSGVO eine Informationspflicht des Verantwortlichen. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, besteht eine Pflicht zur Informationserteilung gemäß Art. 14 Abs. 1 und 2 DSGVO. Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO sehen eine Informationspflicht für den Fall vor, dass der Verantwortliche beabsichtigt, die zuvor (entweder bei der betroffenen oder einer anderen Person) erhobenen personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, als für den sie ursprünglich erhoben wurden. Sofern die Informationen für die Öffentlichkeit bestimmt sind, kann nach Erwägungsgrund 58 der DSGVO die Informationserteilung gemäß Art. 13 und 14 DSGVO über eine Website erfolgen.

§ 48e beschränkt ausschließlich die Informationspflicht gemäß Art. 13 Abs. 3 und Art. 14 Abs. 1, 2 und 4 DSGVO, nicht jedoch jene gemäß Art. 13 Abs. 1 und 2 DSGVO – diese bleibt in vollem Umfang aufrecht.

Die DSGVO sieht in Art. 13 Abs. 4 und Art. 14 Abs. 5 bereits Ausnahmen von der Informationspflicht vor. Jedenfalls kann die Information unterbleiben, wenn die betroffene Person bereits über die Information verfügt. Nach Art. 14 Abs. 5 lit. c DSGVO entfällt die Informationspflicht, wenn die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist. An dieser Stelle ist insbesondere § 48a als eine Maßnahme zum Schutz der Interessen der betroffenen Person zu nennen. Personenbezogene Daten unterliegen im Anwendungsbereich des § 48a der abgabenrechtlichen Geheimhaltungspflicht und dürfen nur in bestimmten Fällen offenbart oder verwertet werden.

Zusätzlich zu den Ausnahmen der DSGVO werden in § 48e den Vorgaben des Art. 23 Abs. 1 DSGVO entsprechende, notwendige und verhältnismäßige Beschränkungen festgelegt. Die Bestimmung gilt gemäß § 2a und § 269 Abs. 1 auch für Verwaltungsgerichte sowie im Rahmen des § 2 lit. b auch in Monopolverfahren.

Die Z 1 sieht im Sinne der in Art. 23 Abs. 1 lit. d bis h DSGVO angeführten Ziele eine Beschränkung der Informationspflicht im Falle einer Gefährdung der Aufgabenerfüllung der Abgabenbehörden oder eines Finanzstrafverfahrens oder eines abgabenrechtlichen Verwaltungsstrafverfahrens vor. Zusätzliche Voraussetzung ist, dass die Interessen der Abgabenbehörden, der Finanzstrafbehörden oder der Bezirksverwaltungsbehörden (als Strafbehörden bei Landes- und Gemeindeabgaben) an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen. Z 1 lit. a bis c enthält eine (demonstrative) Konkretisierung der Gefährdung der Aufgabenerfüllung, wobei alle drei Varianten die Gemeinsamkeit aufweisen, dass durch die Informationserteilung die Ermittlung der tatsächlichen und rechtlichen Verhältnisse, die für die Abgabepflicht und die Erhebung der Abgaben wesentlich sind, maßgeblich erschwert würde.

Z 2 sieht eine durch Art. 23 Abs. 1 lit. c DSGVO gedeckte Beschränkung der Informationspflicht bei Gefährdung der öffentlichen Sicherheit oder Ordnung vor.

Z 3 sieht eine Ausnahme von der Informationspflicht vor, wenn die Informationserteilung den Rechtsträger der Abgabenbehörde (somit den Bund, Länder oder Gemeinden) in der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder in der Verteidigung gegen ihn geltend gemachter zivilrechtlicher Ansprüche beeinträchtigen würde und keine zivilrechtliche Verpflichtung zur Informationserteilung besteht. Das mit der Beschränkung verfolgte Ziel findet in Art. 23 Abs. 1 lit. j DSGVO Deckung.

Z 4 beschränkt die Informationspflicht bei bestimmten Offenbarungen von personenbezogenen Daten, wenn durch die Informationserteilung der Offenbarungszweck vereitelt oder wesentlich beeinträchtigt würde. Vom denkbaren Anwendungsbereich sind daher jedenfalls gemäß § 48a Abs. 4 lit. a und b und gemäß § 48c Z 1 letzter Satz zulässige Offenbarungen erfasst. Darunter können beispielsweise die Verständigung der Finanzstrafbehörde bei Verdacht auf Vorliegen eines Finanzvergehens, die Offenbarung von personenbezogenen Daten zur Aufklärung gerichtlich strafbarer Handlungen oder Verständigungen nach § 48b Abs. 1 oder 2 fallen. Auch im Bereich des internationalen Informationsaustausches hat die Informationserteilung gemäß § 48e Abs. 1 Z 4 zu entfallen, wenn dadurch der Offenbarungszweck (zB Offenbarung zum Zweck der Strafverfolgung durch ausländische Finanzstrafbehörden) gefährdet würde. Hinsichtlich der Informationspflicht gemäß Art. 14 DSGVO kann jedoch in vielen Fällen ohnehin bereits die Ausnahme des Art. 14 Abs. 5 lit. c DSGVO erfüllt sein.

Z 5 normiert den Vorrang gesetzlicher Verschwiegenheitspflichten (zB § 48a, Art. 20 Abs. 3 B-VG).

Z 6 schützt ähnlich dem § 90 Abs. 2 berechtigte Interessen Dritter (Art. 23 Abs. 1 lit. i DSGVO).

Abs. 2 trägt den Vorgaben des Art. 23 Abs. 1 DSGVO Rechnung wonach die Beschränkung notwendig und verhältnismäßig sein muss. Die Notwendigkeit bzw. die Verhältnismäßigkeit der Beschränkung ist aber spätestens dann nicht mehr gegeben, wenn der Grund für die Nichterteilung der Information nachträglich wegfällt und die Informationserteilung möglich und nicht mit einem unverhältnismäßigen Aufwand verbunden ist.

Zu § 48f BAO:

Art. 15 Abs. 1 DSGVO räumt der betroffenen Person das Recht ein, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten. Art. 15 Abs. 3 DSGVO verpflichtet den Verantwortlichen, der betroffenen Person eine Kopie der personenbezogenen Daten zur Verfügung zu stellen.

§ 48f sieht abgabenverfahrensspezifische Beschränkungen des Rechts auf Auskunft gemäß Art. 15 DSGVO vor. Die Beschränkungen entsprechen zum Teil § 26 DSG 2000 sowie § 44 DSG. Die Bestimmung gilt gemäß § 2a und § 269 Abs. 1 auch für Verwaltungsgerichte sowie im Rahmen des § 2 lit. b auch in Monopolverfahren.

§ 48f Abs. 1 Z 1 schränkt das Recht auf Auskunft ein, soweit nach § 48e Abs. 1 Z 1 bis 6 keine Verpflichtung zur Information der betroffenen Person besteht. Die Beschränkungsgründe entsprechen jenen des § 48e.

§ 48f Z 2 sieht als folgerichtige Konsequenz für die nicht im zumutbaren Ausmaß erfolgte Mitwirkung der betroffenen Person am Auskunftsverfahren im Sinne des § 48f Abs. 3 eine Ausnahme vom Auskunftsrecht vor.

Durch § 48f Abs. 2 wird das Verhältnis zwischen dem Auskunftsrecht gemäß Art. 15 DSGVO und der Akteneinsicht gemäß § 90 geregelt. Das Recht auf Auskunft soll – soweit es sich um personenbezogene Daten handelt, die in einem Akt enthalten sind – nicht neben dem Recht auf Akteneinsicht bestehen. Damit wird eine Umgehung der bestehenden Beschränkungen der Akteneinsicht durch das

Auskunftsrecht verhindert. Das Akteneinsichtsverfahren richtet sich ausschließlich nach der BAO – insbesondere nach den §§ 90, 90a und 90b. So ist beispielsweise bei Verweigerung der Akteneinsicht § 90 Abs. 3 zu beachten.

§ 48f Abs. 2 ist in ähnlicher Form in § 44 Abs. 5 DSG bzw. in der bisherigen Regelung des § 28 Abs. 8 DSG 2000 vorgesehen. Sofern man trotz der bestehenden Möglichkeit der Akteneinsicht in § 48f Abs. 2 eine Beschränkung des Auskunftsrechts erblickt, ist diese gerechtfertigt, weil die Akteneinsicht bereits eine durchdachte Abwägung zwischen dem Interesse der Partei an der für sie erforderlichen Informationsbeschaffung einerseits und dem öffentlichen Interesse an einem sparsamen, wirtschaftlichen und zweckmäßigen Verfahren andererseits darstellt (Art. 23 Abs. 1 lit. e DSGVO). Auch Interessen dritter Personen werden im Wege des § 90 Abs. 2 geschützt, was durch Art. 23 Abs. 1 lit. i DSGVO gedeckt ist.

Die betroffene Person kann das Recht auf Auskunft gemäß Art. 15 DSGVO ausüben, wenn § 48f Abs. 1 Z 1 dem Auskunftsrecht nicht entgegensteht und das Auskunftsersuchen personenbezogene Daten betrifft, die nicht in einem Akt enthalten sind. § 48f Abs. 3 normiert wie schon § 26 Abs. 3 DSG 2000 eine Mitwirkungspflicht der betroffenen Person am Auskunftsverfahren. Damit werden der Ausübung des Auskunftsrechtes dort Grenzen gesetzt, wo die Auskunftserteilung einen ungerechtfertigten oder unverhältnismäßigen Aufwand beim Verantwortlichen verursachen würde. Insbesondere wenn der Verantwortliche eine Vielzahl an personenbezogenen Daten über die betroffene Person verarbeitet, hat diese ihr Begehren zweckdienlich zu präzisieren (vgl. auch Erwägungsgrund 63 der DSGVO). Die Beschränkung ist zum Schutz der berechtigten Interessen des Verantwortlichen aber auch im Hinblick auf das öffentliche Interesse an einer sparsamen, wirtschaftlichen und zweckmäßigen Aufgabenerfüllung durch Abgabenbehörden und Verwaltungsgerichte geboten und findet in Art. 23 Abs. 1 lit. e und i DSGVO Deckung.

Im Falle der Nichterteilung der Auskunft gemäß § 48f Abs. 1 Z 1 ist die betroffene Person gemäß Art. 12 Abs. 4 DSGVO darüber zu unterrichten. Diese Unterrichtung hat jedoch nicht in Bescheidform zu erfolgen. Nach § 48f Abs. 4 hat die Begründung der Unterrichtung zu unterbleiben, wenn im Falle einer Nichterteilung der Auskunft gemäß § 48f Abs. 1 Z 1 schon die bloße Kenntnis dieser Gründe durch die betroffene Person ein Zuwiderlaufen des mit der Nichterteilung der Auskunft verfolgten Zweckes zur Folge hätte. Diese Form der Beschränkung ist mit Art. 23 Abs. 2 lit. h DSGVO zu vereinbaren, findet sich auch in § 44 Abs. 3 DSG und war bereits in § 26 Abs. 5 DSG 2000 enthalten.

Im Falle der Nichterteilung der Auskunft gemäß Art. 15 DSGVO ergibt sich aus § 6 des Auskunftspflichtgesetzes, dass die verlangte Auskunft nicht auf das Auskunftspflichtgesetz gestützt werden kann und dass die Verweigerung der Auskunft mangels Anwendbarkeit des § 4 des Auskunftspflichtgesetzes nicht bescheidmäßig erfolgen muss.

Zu § 48g BAO:

Für einen Verantwortlichen besteht nach der DSGVO die Pflicht zur Berichtigung, Aktualisierung oder Vervollständigung (im Folgenden „Berichtigung“) von durch ihn verarbeitete personenbezogene Daten. Diese Pflicht ergibt sich einerseits direkt aus Art. 5 Abs. 1 lit. d DSGVO, andererseits aus dem Recht der betroffenen Person gemäß Art. 16 DSGVO.

Der Rechtskraft fähige Erledigungen wie Bescheide der Abgabenbehörde und Erkenntnisse oder Beschlüsse des Verwaltungsgerichts aber auch Selbstberechnungen enthalten personenbezogene Daten. Diese personenbezogenen Daten unterliegen grundsätzlich einer Pflicht zur Berichtigung im Sinne der Bestimmungen der DSGVO. Da diese Pflicht zur Berichtigung mit dem Rechtskraftkonzept der BAO in einem Spannungsverhältnis steht, muss sie beschränkt werden. Aus diesem Grund enthält § 48g Beschränkungen der Berichtigungspflicht. Die Bestimmung gilt gemäß § 2a und § 269 Abs. 1 auch für Verwaltungsgerichte sowie im Rahmen des § 2 lit. b auch in Monopolverfahren.

Aufgrund der Ausnahmeregelung des § 48g Abs. 1 kann an sämtlichen bestehenden abgabenverfahrensrechtlichen Regelungen über die Berichtigung, Abänderung, Zurücknahme oder Aufhebung in den genannten Fällen festgehalten werden. Insbesondere wird an der Rechtskraft von Bescheiden bzw. an der Verjährung nichts geändert.

Als denkbare Maßnahmen, um personenbezogene Daten eines Bescheides zu berichtigen, kommen neben § 293, § 293a und § 293b beispielsweise auch eine Beschwerdevorentscheidung, ein Erkenntnis oder die Aufhebung des Bescheides samt Erlassung einer neuen Sachentscheidung in Betracht (zB § 299, § 307). Im Zusammenhang mit Selbstberechnungen kann eine Berichtigung im Wege der Erlassung eines Bescheides gemäß § 201 erfolgen.

Die durch § 48g Abs. 1 erreichte Wahrung der Rechtssicherheit und Rechtsbeständigkeit stellt ein wichtiges öffentliches Interesse dar; die Einschränkung des Berichtigungsrechts ist daher von Art. 23

Abs. 1 lit. e DSGVO gedeckt. Sie dient weiters auch dem Schutz der betroffenen Person und dem Schutz der Rechte und Freiheiten anderer Personen und ist daher von Art. 23 Abs. 1 lit. i DSGVO gedeckt. Darüber hinaus wird (zB durch § 302) der Eintritt von Rechtsfrieden sichergestellt und Beweisschwierigkeiten im Zusammenhang mit der Überprüfung der Richtigkeit von Daten angesichts lange verstrichener Zeit vorgebeugt.

Ist jedoch eine Berichtigung nach den Abgabenvorschriften zulässig und liegt sie im Ermessen der Abgabenbehörde, wird dem Interesse der betroffenen Person an der Richtigkeit der sie betreffenden personenbezogenen Daten insofern Rechnung getragen, als nach der ständigen Judikatur des VwGH grundsätzlich dem Prinzip der Rechtmäßigkeit (Rechtsrichtigkeit) der Vorrang vor dem Prinzip der Rechtssicherheit (Rechtsbeständigkeit) zukommt (zB VwGH 30.1.2001, 99/14/0067; 14.12.2006, 2002/14/0022; 28.5.2009, 2007/15/0285). Eine Berichtigung wird daher in diesen Fällen in der Regel zu erfolgen haben.

§ 48g Abs. 2 regelt jene Fälle, in denen die aufgrund der DSGVO erforderliche Berichtigung möglich ist und dafür kein rechtsförmliches Verfahren erforderlich (Abs. 1) ist. In diesen Fällen kann die Erforderlichkeit der Berichtigung mit der Notwendigkeit der Nachvollziehbarkeit einzelner Schritte im Verfahren in einem Spannungsverhältnis stehen. Ist daher die Berichtigung personenbezogener Daten als nachträgliche Änderung mit dem Zweck der Nachvollziehbarkeit der ursprünglichen Angaben nicht zu vereinbaren, hat sie im Wege eines ergänzenden Vermerks zu erfolgen. Dies betrifft beispielsweise zu berichtigende Daten eines Aktenvermerks oder einer Auskunft der Abgabenbehörde.

Enthalten die BAO oder andere Abgabenvorschriften für bestimmte Berichtigungsfälle spezifische Bestimmungen, so gehen diese dem § 48g Abs. 2 vor. Beispielsweise gilt für Niederschriften § 87 Abs. 5. Ein weiteres Beispiel für eine spezifische Bestimmung ist, dass eine Berichtigung, die eine Abänderung von Rechten und Pflichten zur Folge hätte (zB die Berichtigung von falschen personenbezogenen Daten in einer Abgabenerklärung) aufgrund von § 92 Abs. 1 zwingend durch einen Bescheid (bzw. gemäß § 198 Abs. 1 durch einen Abgabenbescheid) zu erfolgen hat. Ein Beispiel für eine spezifische Berichtigungsbestimmung in einer anderen Abgabenvorschrift ist § 15 Abs. 1 AbgEO.

§ 48g Abs. 3 beschränkt für das Abgaben- und Beschwerdeverfahren das Recht einer betroffenen Person gemäß Art. 18 Abs. 1 lit. a DSGVO vom Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die Richtigkeit der personenbezogenen Daten von ihr bestritten wird. Dieses Recht wird allerdings nur für jene Fälle eingeschränkt, in denen sich bei der Überprüfung der Richtigkeit durch die Abgabenbehörde weder die Richtigkeit noch die Unrichtigkeit der personenbezogenen Daten feststellen lässt. Ohne diese Einschränkung könnte aufgrund der DSGVO für diese Fälle die dauerhafte Einschränkung der Verarbeitung begehrt werden, was einem wichtigen Ziel des öffentlichen Interesses (nämlich der Durchführbarkeit des Abgabenverfahrens und der Gleichmäßigkeit der Besteuerung) entgegenstünde. Daher ist diese Einschränkung von Art. 23 Abs. 1 lit. e DSGVO gedeckt.

Die Bestimmung gilt gemäß § 2a und § 269 Abs. 1 auch für Verwaltungsgerichte sowie im Rahmen des § 2 lit. b auch in Monopolverfahren.

Zu § 48h BAO:

Es gibt einige Fälle, in denen juristische oder natürliche Personen aufgrund abgabenrechtlicher Bestimmungen personenbezogene Daten verarbeiten und in diesem Zusammenhang als Verantwortliche im Sinn der DSGVO anzusehen sind. Da sie keine Abgabenbehörden sind, sollen die datenschutzrechtlichen Sonderbestimmungen der BAO, soweit ihnen abgabenrechtliche Aufgaben übertragen wurden, ausdrücklich auf sie anwendbar gemacht werden. Gemeint sind damit beispielsweise:

- Parteienvertreter, denen im Hinblick auf die Selbstberechnung und Entrichtung der Immobilienertragsteuer oder der Grunderwerbsteuer Pflichten zur Datenverarbeitung auferlegt sind (zB durch § 30c Abs. 1 EStG 1988 oder durch § 13 Abs. 1 GrEStG 1987).
- Arbeitgeber, denen im Hinblick auf die Berechnung, Einbehaltung und Abfuhr der Lohnsteuer Pflichten zur Datenverarbeitung auferlegt sind (zB durch § 76 EStG 1988).
- Abzugsverpflichtete, denen im Hinblick auf die Berechnung, Einbehaltung und Abfuhr der Kapitalertragsteuer Pflichten zur Datenverarbeitung auferlegt sind (zB durch § 96 Abs. 4 EStG 1988).
- Abzugsverpflichtete, denen im Hinblick auf die Berechnung, Einbehaltung und Abfuhr der im Wege einer Abzugsteuer zu erhebenden Einkommensteuer beschränkt Steuerpflichtiger Pflichten zur Datenverarbeitung auferlegt sind (zB durch § 101 Abs. 2 EStG 1988).

Zu § 48i BAO:

§ 14 Abs. 5 DSG 2000 sah 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 weder die DSGVO noch die BAO eine entsprechend spezifische Regelung enthalten, wird in § 48i – als Datensicherheitsmaßnahme – die Aufbewahrungsdauer von Protokolldaten wie bereits in § 14 Abs. 5 DSG 2000 mit drei Jahren festgelegt, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist. Wenn daher nach der DSGVO über tatsächlich durchgeführte Verarbeitungsvorgänge Protokoll zu führen ist, kann insbesondere die Überprüfung der Zugriffsberechtigung von Personen, die auf den protokollierten Datenbestand zugegriffen haben, weiterhin gewährleistet werden. Nach Ablauf von drei Jahren besteht gemäß Art. 17 DSGVO eine Löschungsverpflichtung, soweit nicht eine Ausnahme nach Art. 17 Abs. 3 DSGVO vorliegt.

Zu Art. 70 Z 3 und 4 (§ 97 Abs. 3 und § 97a Z 1 BAO):

Die beiden Bestimmungen enthielten Verweise auf das Datenschutzgesetz 2000 im Allgemeinen. Das Datenschutzrecht wurde bisher ausschließlich durch das Datenschutzgesetz 2000 geregelt. Seit dem Inkrafttreten der DSGVO wird das Datenschutzrecht nunmehr durch mehrere unterschiedliche Rechtsvorschriften geregelt, vor allem durch die DSGVO selbst, das Datenschutzgesetz in der Fassung des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, und verschiedene weitere gesetzliche Bestimmungen. Der in § 97 Abs. 3 und § 97a Z 1 verwendete Begriff „Datensicherheit“ ist in einer Zusammenschau der einschlägigen datenschutzrechtlichen Bestimmungen auszulegen.

Zu Art. 70 Z 5 (§ 114 Abs. 4 BAO):

Der Regelungsinhalt des derzeit geltenden § 114 Abs. 4 wird teilweise durch die neue Bestimmung des § 48d abgedeckt. Insoweit der geltende § 114 Abs. 4 eine Rechtsgrundlage für die Datenverarbeitung zum Zweck der Betrugsbekämpfung oder des automationsunterstützten Risikomanagements dargestellt hat, wird er unter Berücksichtigung der aktuellen datenschutzrechtlichen Terminologie neu gefasst. Unter automationsunterstütztes Risikomanagement fällt unter anderem die softwaregestützte Analyse von Daten mit Predictive-Analytics-Methoden oder die Datenanalyse im Vorfeld von Kontroll- und Prüfungshandlungen. Unter dem Begriff „Betrugsbekämpfung“ sind alle Maßnahmen zur Verhinderung, Aufdeckung und Verfolgung von Zuwiderhandlungen gegen die von Abgabenbehörden zu vollziehenden Rechtsvorschriften zu verstehen.

Zu Art. 70 Z 6 (§ 323 Abs. 53 BAO):

Das Inkrafttreten der datenschutzrechtlichen Bestimmungen der BAO erfolgt gleichzeitig mit dem Inkrafttreten der DSGVO und des Datenschutzgesetzes in der Fassung des Bundesgesetzes BGBl. I Nr. 120/2017.

Zu Art. 71 (Änderung der Abgabenexekutionsordnung)

Zu Z 1 (§ 25 Abs. 3 AbgEO):

Durch diese Bestimmung wird das Verhältnis zwischen dem Auskunftsrecht gemäß Art. 15 DSGVO und der Akteneinsicht gemäß § 25 Abs. 1 geregelt. Das Recht auf Auskunft soll nicht neben dem Recht auf Akteneinsicht bestehen. Damit wird eine Umgehung der bestehenden Beschränkungen der Akteneinsicht durch das Auskunftsrecht verhindert. Das Akteneinsichtsverfahren richtet sich nach der AbgEO bzw. ergänzend nach den Bestimmungen der BAO.

§ 25 Abs. 3 ist in ähnlicher Form in § 44 Abs. 5 DSG bzw. in der bisherigen Regelung des § 28 Abs. 8 DSG 2000 vorgesehen. Sofern man trotz der bestehenden Möglichkeit der Akteneinsicht in Abs. 3 eine Beschränkung des Auskunftsrechts erblickt, ist diese gerechtfertigt, weil die Akteneinsicht bereits eine durchdachte Abwägung zwischen dem Interesse der Partei an der für sie erforderlichen Informationsbeschaffung einerseits und dem öffentlichen Interesse an einem sparsamen, wirtschaftlichen und zweckmäßigen Verfahren andererseits darstellt (Art. 23 Abs. 1 lit. e DSGVO).

Zu Z 2 (§ 44 Abs. 6 AbgEO):

Die Bestimmung enthielt einen Verweis auf das Datenschutzgesetz 2000 im Allgemeinen. Das Datenschutzrecht wurde bisher ausschließlich durch das Datenschutzgesetz 2000 geregelt. Seit dem Inkrafttreten der DSGVO wird das Datenschutzrecht nunmehr durch mehrere unterschiedliche Rechtsvorschriften geregelt, vor allem durch die DSGVO selbst, das Datenschutzgesetz in der Fassung des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, und verschiedene weitere gesetzliche

Bestimmungen. Der in § 44 verwendete Begriff „personenbezogene Daten“ ist in Art. 4 Z 1 DSGVO definiert.

Zu Z 3 (§ 90a Abs. 13 AbgEO):

Das Inkrafttreten der datenschutzrechtlichen Bestimmungen der AbgEO erfolgt gleichzeitig mit dem Inkrafttreten der DSGVO und des Datenschutzgesetzes in der Fassung des Bundesgesetzes BGBl. I Nr. 120/2017.

Zu Art. 72 (Änderung des Finanzstrafgesetzes)

Zu Art. 72 Z 2 (§§ 57a, 57b, 57c und 57d FinStrG):

§ 57a:

Die Datenschutz-RL wurde mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, im dritten Hauptstück des DSG umgesetzt. Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausdrücklich klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. So sind etwa Regelungen über Akteneinsicht oder Verständigungspflichten als leges speciales zum 3. Hauptstück zu beurteilen.

Der Vollzug der Bestimmungen des Finanzstrafgesetzes erfordert zu einem großen Teil die Verarbeitung personenbezogener Daten. Im Sinne der Rechtssicherheit soll die Umsetzung der Datenschutz-RL für den Bereich des Finanzstrafrechts weitgehend im Finanzstrafgesetz erfolgen. Bestimmungen des dritten Hauptstücks des DSG, die nicht Besonderheiten des Finanzstrafverfahrens betreffen, wie beispielsweise die Pflichten des Verantwortlichen oder die Bestimmungen über die Aufsichtsbehörde, sollen jedoch nicht eigenständig geregelt werden. Die Protokollierungspflicht für Papierakten gemäß § 50 Abs. 3 DSG soll ausgenommen werden, da eine solche in der Datenschutz-RL nicht vorgesehen ist und die Aktenführung bereits entsprechenden Vorgaben unterliegt. Die Einschränkung der Anwendbarkeit der §§ 58 und 59 DSG entspricht Art. 61 der Datenschutz-RL.

Abs. 2 stellt eine allgemeine Ermächtigungsnorm dar.

Abs. 3 regelt die Weiterverarbeitung von Daten, die für einen bestimmten finanzstrafrechtlichen Zweck oder sonst zur Erfüllung einer bestimmten Aufgabe erhoben oder erfasst wurden und in weiterer Folge für die Erfüllung einer anderen Aufgabe verarbeitet werden.

Gemäß Abs. 4 sollen personenbezogene Daten, die auf persönlichen Einschätzungen beruhen, als solche erkennbar sein.

In Abs. 5 sind unter „besondere Kategorien personenbezogener Daten“ Daten im Sinne des § 39 DSG zu verstehen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die in Art. 10 der Datenschutz-RL diesbezüglich geforderten, geeigneten Garantien für die Ermächtigungsnorm des Abs. 5 sind in Anbetracht der verfahrensrechtlichen und organisatorischen Maßnahmen aufgrund der abgabenrechtlichen Geheimhaltungspflicht (§ 48a Bundesabgabenordnung) gegeben.

In Hinblick auf die Aufsichtsbehörde sollen die Bestimmungen des 4. Abschnitts des DSG sinngemäß anzuwenden sein. Im Einklang mit Art. 45 Abs. 2 der Datenschutz-RL und § 31 Abs. 1 DSG soll die Datenschutzbehörde nicht für die Aufsicht über die entsprechenden von den Spruchsenaten oder vom Bundesfinanzgericht im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Datenverarbeitungen zuständig sein.

Im Falle der Verarbeitung personenbezogener Daten, die nicht in den Anwendungsbereich der Datenschutz-RL fallen, weil die jeweilige Verarbeitung nicht für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung vorgenommen wird, sollen die Bestimmungen der Datenschutz-Grundverordnung nach Maßgabe der entsprechenden Bestimmungen der Bundesabgabenordnung gelten.

§ 57b:

In Entsprechung des Art. 18 der Datenschutz-RL sollen die Betroffenenrechte im Einklang mit den Bestimmungen des Finanzstrafgesetzes geregelt werden. Die bereits bestehenden verfahrensrechtlichen Verständigungspflichten sollen durch das Bereitstellen entsprechender Angaben auf der Homepage ergänzt werden. Die Bestimmungen zur Akteneinsicht gelten – wie im Bericht des

Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausgeführt – als leges speciales zu den datenschutzrechtlichen Vorgaben. Abs. 2 dient daher einer entsprechenden Klarstellung.

§ 57c:

Das Recht auf Berichtigung ist im Strafverfolgungskontext nur eingeschränkt durchsetzbar. So sind davon keine nachträglichen Änderungen von Vernehmungen umfasst; hier bezieht sich die Richtigkeit und Vervollständigung der personenbezogenen Daten auf die Übereinstimmung mit der Aussage selbst und nicht auf deren Inhalt. Gleiches gilt für Beweismittel anderer Art. Daher soll das Recht auf Berichtigung gemäß Art. 18 der Datenschutz-RL im Einklang mit dem innerstaatlichen Recht geregelt werden. Im Falle behördlicher Erledigungen, dazu gehören insbesondere Bescheide, verfahrensleitende Verfügungen und Erkenntnisse, sowie für Niederschriften besteht das Recht auf Berichtigung nur nach Maßgabe der für das Finanzstrafverfahren geltenden allgemeinen Verfahrensvorschriften. So sind zum Beispiel Unrichtigkeiten in einer Niederschrift durch entsprechende Ergänzungen richtig zu stellen (§ 56 Abs. 2 FinStrG in Verbindung mit § 87 Abs. 5 BAO). Eine Berichtigung setzt überdies die objektive Feststellung der tatsächlichen Unrichtigkeit oder Unvollständigkeit durch die Behörde voraus. Eine Unmöglichkeit der Berichtigung kann insbesondere in technischer Hinsicht bestehen.

§ 57d:

Weiters sollen im Einklang mit Art. 5 und Art. 18 der Datenschutz-RL geeignete Fristen für die Löschung oder die Überprüfung der Notwendigkeit der Speicherung personenbezogener Daten sowie allfälliger Protokolldaten vorgesehen werden.

Zu Art. 72 Z 3 (§ 80 FinStrG):

Die Ergänzungen sollen der Klarstellung und Anpassung an datenschutzrechtliche Erfordernisse dienen.

Zu Art. 72 Z 4 (§ 120 FinStrG):

Die Anpassung soll der Änderung des Datenschutzrechts Rechnung tragen. Weiters soll klargestellt werden, dass auch der Bundesminister für Finanzen in seiner Funktion als Dienstaufsichtsbehörde sowie zur Erfüllung der ihm durch dieses Bundesgesetz zugewiesenen Aufgaben die entsprechenden Datenbankabfragen vornehmen darf.

Mit dem neuen Abs. 5 soll klargestellt werden, dass personenbezogene Daten, die zur Durchführung von Abgaben- oder Monopolverfahren erforderlich sind, an die Abgabenbehörden zu übermitteln sind.

Zu Art. 72 Z 5 (§ 194c FinStrG):

Aufgrund der neuen datenschutzrechtlichen Bestimmungen soll der bisherige Abs. 1 angepasst werden und die Verpflichtung zur Löschung unzulässiger Weise aufgenommener Daten in den Abs. 2 verschoben werden.

Zu Art. 72 Z 6 (§ 194d Abs. 3 FinStrG):

Der bisherige Verweis auf das Datenschutzgesetz soll angepasst werden.

Zu Art. 72 Z 7 (§ 194e Abs. 2 FinStrG):

Dem Entfall des Begriffs „Dienstleister“ soll Rechnung getragen werden.

Zu Art. 72 Z 8 (§ 195 FinStrG):

Die besonderen datenschutzrechtlichen Bestimmungen dieses Bundesgesetzes sollen für die Verarbeitung von Daten, die durch die Finanzstrafbehörden, die für sie tätigen Organe und den Bundesminister für Finanzen vorgenommen wird, auch für Daten sinngemäß anzuwenden sein, die im Zuge gerichtlicher Ermittlungen verarbeitet werden. Somit soll innerhalb der Finanzverwaltung eine einheitliche Vorgangsweise zur Verarbeitung personenbezogener Daten gewährleistet werden.

Zu Art. 72 Z 9 (§ 257 FinStrG):

Die Datenschutz-RL soll für den Bereich des Finanzstrafrechts im Wesentlichen in diesem Bundesgesetz umgesetzt werden.

Zu Art. 72 Z 10 (§ 265 FinStrG):

Laut Art. 63 der Datenschutz-RL ist diese von den Mitgliedstaaten bis zum 6. Mai 2018 umzusetzen. Aufgrund der Inkrafttretensbestimmungen des § 70 DSG in der Fassung des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, sollen auch die entsprechenden Bestimmungen des FinStrG erst mit 25. Mai 2018 Inkrafttreten.

Zum 7. Hauptstück (Inneres)

Allgemeines:

Aufgrund der neuen datenschutzrechtlichen Vorgaben haben die gesetzlich geregelten Datenverarbeitungen ab dem 25. Mai 2018 den durch die DSGVO und die Datenschutz-RL geänderten Anforderungen zu genügen, weshalb nahezu sämtliche Materiengesetze, die in den legistischen Zuständigkeitsbereich des Bundesministeriums für Inneres fallen, anzupassen sind. Da gemäß § 69 Abs. 8 DSG – im Rahmen der europa- und verfassungsrechtlichen Vorgaben – vom DSG abweichende Regelungen in Bundes- und Landesgesetzen zulässig sind, sollen die einschlägigen materienspezifischen Regelungen im Bereich des Datenschutzes als leges speciales den allgemeinen Regelungen des neuen DSG vorgehen.

Das in der DSGVO vorgesehene Recht auf Widerspruch oder auf Einschränkung der Verarbeitung steht in einem Spannungsverhältnis zur gesetzlich angeordneten Datenverarbeitung. Durch die Ausübung dieser Rechte könnte ein Betroffener verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben zumindest für die Dauer der Prüfung des Antrages verarbeitet werden dürfen.

Gemäß Art. 23 DSGVO kann zur Sicherstellung einer der in Abs. 1 lit. a bis j genannten Zwecke durch nationale Bestimmungen das Widerspruchsrecht und das Recht auf Einschränkung der Verarbeitung beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Die in dieser Bestimmung genannten Gründe für die Zulässigkeit des Ausschlusses dieser Rechte sind auch vor dem Hintergrund der im Verfassungsrang stehenden Bestimmung des § 1 Abs. 2 DSG zu sehen, wonach Eingriffe einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 EMRK genannten Gründen zulässig sind, vorgenommen werden dürfen. Danach ist ein Eingriff einer staatlichen Behörde nur dann statthaft, wenn dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. Damit zeigt sich, dass gesetzlich vorgesehene Eingriffe, die im Einklang mit der Verfassung stehen, jedenfalls die Voraussetzungen mit sich bringen, die für die Zulässigkeit einer Beschränkung gemäß Art. 23 Abs. 1 DSGVO erforderlich sind.

Für den geordneten Vollzug der maßgeblichen Materien, wie etwa des Melderechts, des Personenstandsrechts oder des Wahlrechts, ist es unerlässlich, dass Daten des Betroffenen weiterverarbeitet werden dürfen. Es kann nicht dem Betroffenen anheimgestellt sein, durch die Ausübung dieser Rechte etwa zu verhindern, dass die Fremdenpolizei nicht über ein aufrechtes Aufenthaltsverbot oder die gesamte staatliche Verwaltung über den Wohnsitzwechsel informiert werden dürfen. Im Hinblick auf das Zentrale Melderegister ist überdies noch anzumerken, dass mit der Inanspruchnahme dieses Rechts die im E-Government-Gesetz vorgesehene elektronische Abwicklung von Verwaltungsvorgängen verunmöglicht würde.

Wenn in Art. 23 Abs. 2 DSGVO für einschränkende Maßnahmen vorgeschrieben wird, dass diese spezifische Vorschriften zu enthalten haben, ist davon auszugehen, dass es sich dabei um Maßnahmen handelt, die spätestens seit dem DSG 2000 zum notwendigen Standard für jede gesetzliche Maßnahme, die den Eingriff in das Recht auf Schutz der personenbezogenen Daten erlaubt, gehören. Eine Ergänzung war nur insoweit vorzusehen, als Betroffene über diese Einschränkung zu informieren sind.

Der Ausschluss des Rechts auf Einschränkung der Verarbeitung und des Widerspruchsrechts führt aber nicht dazu, dass der Betroffene inhaltlich eine Beschränkung dahingehend erfährt, dass er sich nicht gegen die Verarbeitung unrichtiger Daten oder gegen eine unrechtmäßige Verarbeitung zur Wehr setzen könnte. Das Recht auf Berichtigung und das Recht auf Löschung bleiben davon natürlich unberührt.

Mit diesem Gesetzesvorschlag werden auch die Grundlagen dafür vorgeschlagen, die bisherigen Informationsverbundsysteme den Vorgaben der DSGVO anzupassen. Dabei stellt sich die besondere Herausforderung, dass die bislang in Österreich geltende Rechtslage eine Systematik für diesen Bereich (§ 50 DSG 2000) vorsah, die sich in dieser Weise in der DSGVO nicht mehr findet. Art. 26 DSGVO sieht nur die Möglichkeit vor, dass zwei oder mehr Verantwortliche gemeinsam Daten verarbeiten dürfen. Dazu haben sie in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtungen gemäß dieser Verordnung erfüllt. Eine solche Vereinbarung ist jedoch nicht erforderlich, wenn die jeweiligen Aufgaben der Verantwortlichen durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt sind. Mit dem vorliegenden Gesetzesvorschlag soll daher auf Gesetzesebene die Aufgabenverteilung bei der gemeinsamen Verarbeitung im Bereich der bisherigen Informationsverbundsysteme festgelegt werden, sodass eine vertragliche Vereinbarung entfallen kann.

Verantwortliche im Sinne der Unionsvorschrift sollen dabei die bisherigen Auftraggeber der Informationsverbundsysteme sein. In den gesetzlichen Regelungen wird zwar sowohl der Zweck der Datenverarbeitung als auch das Mittel, nämlich eine bestimmte zentrale Anwendung (zB das ZMR), festgelegt, obwohl die DSGVO den Verantwortlichen grundsätzlich dadurch gekennzeichnet sieht, als eben dieser Zweck und Mittel festlegt. Die vorliegenden Regelungen orientieren sich daher daran, dass nach Art. 4 Z 7 DSGVO, wenn Zweck und Mittel durch das Recht der Mitgliedstaaten vorgesehen werden, der Verantwortliche oder die Kriterien der Benennung des Verantwortlichen auch nach diesem Recht vorgenommen werden können. In den hier gegenständlichen Fällen wird die jeweils zur Vollziehung der jeweiligen Materie zuständige Behörde als Verantwortliche bezeichnet, die die Entscheidung über die konkrete Datenverarbeitung trifft. Insoweit ist davon auszugehen, dass die vorgeschlagenen Regelungen mit dem Unionsrecht jedenfalls im Einklang stehen.

Schon bisher war der Bundesminister für Inneres in einem Großteil der von dieser Gesetzesinitiative betroffenen Informationsverbundsysteme als Betreiber und Dienstleister vorgesehen. Die Rolle des Betreibers war zur Gänze zu streichen. Hinsichtlich der Funktion als Dienstleister oder als Auftragsverarbeiter, wie diese Funktion in der DSGVO bezeichnet wird, ist vor dem verfassungsrechtlichen Hintergrund, dass der Bundesminister für Inneres oberstes Organ ist, nicht zu übersehen, dass ein Spannungsverhältnis vermutet werden könnte, da es zum Wesen eines Auftragsverarbeiters gehört, dass er nur im Auftrag oder nur mit Genehmigung des Verantwortlichen tätig wird (Art. 28 DSGVO). Verfassungswidrig wäre es, wenn vorgesehen würde, dass der Bundesminister in dieser Rolle an Willensbildungen anderer Stellen, also etwa der nachgeordneten Behörden als Verantwortliche gebunden sein würde. Die vorgeschlagenen Regelungen sehen Derartiges nicht vor. Vielmehr erfolgt die Beauftragung und Bindung ausschließlich durch das Gesetz selbst. Dabei werden dem Bundesminister für Inneres in erster Linie Aufgaben übertragen, wie sie typischerweise einem Auftragsverarbeiter gemäß Art. 28 DSGVO zukommen, die eben – wie dies dort auch als zulässig erachtet wird – nicht im Rahmen eines Vertrages übertragen werden, sondern durch ein Rechtsinstrument des Mitgliedstaates, hier ein Gesetz. Insoweit kommt ihm aber auch nicht die Rolle eines Verantwortlichen zu, da er in keiner Weise die Entscheidung über die Verarbeitung der Daten trifft. Diese Entscheidung kommt allein den Verantwortlichen zu. Wie dies bereits in den Erläuterungen zum DSG 1978 ausgeführt wird, ändern auch die im öffentlichen Bereich bestehenden Weisungen an nachgeordnete Organe, im Rahmen ihrer Eigenzuständigkeit Datenverarbeitungen einzusetzen, nichts daran; dabei handelt es sich nicht um solche Aufträge, wie sie sich im Verhältnis von Auftraggeber und Dienstleister – oder in der Terminologie der DSGVO von Verantwortlichem und Auftragsverarbeiter – darstellen. Diese Weisungen bilden nämlich nicht den unmittelbaren Anlass für die Aufnahme der Datenverarbeitung; sie wird vielmehr erst durch entsprechende Akte des angewiesenen Organs bewirkt (vgl. ErläutRV 554 BlgNR 16. GP 13).

Damit wird durch die vorgesehene Einbindung des Bundesministers für Inneres weder in die Position als oberstes Organ, noch in den geltenden Weisungszusammenhang eingegriffen.

Entsprechendes ist auch für den Anwendungsbereich der DS-RL durch die Bestimmungen des Art. 21 DS-RL bzw. § 47 DSG für die gemeinsame Verarbeitung vorgegeben.

Zu Art. 73 (Änderung des Bundes-Stiftungs- und Fondsgesetzes 2015)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 13 B-VG („Stiftungs- und Fondswesen, soweit es sich um Stiftungen und Fonds handelt, die nach ihren Zwecken über den Interessenbereich eines Landes hinausgehen und nicht schon bisher von den Ländern autonom verwaltet wurden“).

Zu Art. 73 Z 1 (§ 22 Abs. 2a):

Da die DSGVO (Art. 4 Z 10) „Dritten“ eine andere Bedeutung zugrunde legt, soll eine terminologische Anpassung erfolgen. Dadurch soll sich jedoch keine inhaltliche Änderung im Vergleich zur geltenden Rechtslage ergeben.

Zu Art. 73 Z 2 und 3 (§ 22 Abs. 3, § 28 Abs. 2):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Zu Art. 74 (Änderung des Gedenkstättengesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 13 B-VG („Angelegenheiten der künstlerischen und wissenschaftlichen Sammlungen und Einrichtungen des Bundes“) und auf Art. 17 B-VG (Angelegenheiten der Privatwirtschaftsverwaltung).

Zu Art. 74 Z 1 bis 4 (§ 29):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Dem „Auftraggeber“ (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und deckt sich daher mit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie das in der DSGVO normierte Transparenzgebot (vgl. ErwGr 60 zur DSGVO; siehe auch Art. 5 DSGVO), soll durch den Verweis in Abs. 2 auf § 3 die Klarstellung erfolgen, was unter den übertragenen Aufgaben zu verstehen ist.

Da die DSGVO den Terminus Weitergabe nicht kennt, kann dieser in Abs. 3 entfallen.

§ 14 DSG 2000 sieht 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. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. Im Hinblick auf den Entfall des bisherigen § 14 DSG 2000 zufolge des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, und den Umstand, dass die DSGVO von spezifischen Regelungen betreffend die Protokollierung Abstand nimmt, wird vorgeschlagen, in Abs. 4 eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Zu Art. 75 (Änderung des Meldegesetzes 1991)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Meldewesen“).

Zu Art. 75 Z 3 (§ 4 Abs. 4 und § 4a Abs. 2 MeldeG):

Es soll die Klarstellung erfolgen, dass es sich um die Amtssignatur des Bundesministers für Inneres handelt.

Zu Art. 75 Z 4, 5, 6, 8, 9, 10, 17, 19, 24, 25, 26, 28, 30, 32, 33, 34 und 35 (§ 4a Abs. 1 [idF BGBl. I Nr. 120/2016], § 4a Abs. 3, § 11 Abs. 3, Überschrift zum 2. Abschnitt, § 14 Abs. 1, 1a und 4, § 16 Abs. 5 bis 7, Überschrift zu § 16a, § 16a Abs. 6, § 16b Abs. 2 und 4, § 16c, § 17 Abs. 5, § 20 Abs. 1 und 3 MeldeG):

Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im Meldegesetz verwendeten Begriffe erforderlich erscheint, sollen diese an die Definitionen der DSGVO (Art. 4 DSGVO) angeglichen werden. Beispielsweise sollen die Begriffe „überlassen“, „mitteilen“, „zur Verfügung stellen“, das „Weitergeben“ oder das „Weiterleiten“ von Daten durch „übermitteln“ ersetzt werden. Dem „Auftraggeber“ (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der „Auftragsverarbeiter“ (§ 4 Z 8 DSGVO) deckt sich grundsätzlich mit dem bisherigen „Dienstleister“ im Sinne des DSG 2000.

Soweit es sich hingegen bei der Datenanwendung um ein Informationsverbundsystem handelt, entspricht der Auftragsverarbeiter im Sinne der DSGVO dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Melderegister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht

damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Zu Art. 75 Z 7 und 12 (Überschrift zu § 14, Überschrift zu § 15 MeldeG):

Die Änderungen dienen der Anpassung an den Gesetzestext.

Zu Art. 75 Z 11 und 27 (§ 14 Abs. 5, § 16a Abs. 12 MeldeG):

§ 14 DSG 2000 sieht 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. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. 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, im Rahmen des lokalen Melderegisters in Abs. 5 eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Zu Art. 75 Z 13 (§ 15 Abs. 1a MeldeG):

Es handelt sich um eine terminologische Anpassung.

Zu Art. 75 Z 14 (Überschrift zu § 16 MeldeG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO.

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Dieser hat daher in der Überschrift zu § 16 zu entfallen

Zu Art. 75 Z 15 (§ 16 Abs. 1 und 2 MeldeG):

Zu Abs. 1:

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Art. 26 DSGVO sieht stattdessen vor, dass wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 16 Abs. 1 entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der im Zentralen Melderegister verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden. Zudem sollen die Meldebehörden wie bisher (Abs. 2) verpflichtet sein, dem Bundesminister für Inneres für Zwecke der Führung des Zentralen Melderegisters ihre Meldedaten zu übermitteln.

Die Festlegung des ZMR als öffentliches Register ist im Hinblick auf § 17 Abs. 2 Z 2 DSG 2000 relevant, wonach öffentliche Register als Datenanwendungen nicht der Meldepflicht gegenüber der Datenschutzbehörde unterliegen. Mit Inkrafttreten des Datenschutz-Anpassungsgesetzes 2018 entfällt die gegenständliche Meldung, weshalb die Klarstellung, dass es sich um ein öffentliches Register handelt, künftig nicht mehr erforderlich ist.

Zusätzlich soll im letzten Satz die Klarstellung erfolgen, dass es sich um das bPK für die Verwendung im privaten Bereich (§ 14 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) handelt.

Soweit personenbezogene Daten durch Evidenzstellen gemäß § 51 Staatsbürgerschaftsgesetz 1985 (StbG), BGBl. Nr. 311/1985, sowie durch Personenstandsbehörden im Sinne des Personenstandsgesetzes 2013 (PStG 2013), BGBl. I Nr. 16/2013, an das Zentrale Melderegister übermittelt werden (§ 11 Abs. 1 und Abs. 1a MeldeG, § 12 und § 31 PStG 2013), sollen diese für die Meldebehörden als Auftragsverarbeiter tätig werden. Gleiches gilt für Behörden gemäß § 16 Abs. 3, die personenbezogene Daten in Häftlingsevidenzen verarbeiten und diese an das Zentrale Melderegister zum Zwecke der Verarbeitung für die Meldebehörden übermitteln.

Zu Abs. 2

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen

Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 2 die Zuständigkeit zwischen den gemeinsam Verantwortlichen des Zentralen Melderegisters dahingehend aufteilen, dass Informations-, Auskunfts-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiges Recht nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher wie hier eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Zu Art. 75 Z 16 (§ 16 Abs. 2a MeldeG):

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung derzeit um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Melderegister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Zudem soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Art. 75 Z 17 (§ 16 Abs. 5 MeldeG):

Aufgrund der datenschutzrechtlichen Anpassungen kann der Verweis auf Abs. 2 entfallen.

Zu Art. 75 Z 18 (§ 16 Abs. 8 MeldeG):

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 § 16 Abs. 8 für sämtliche nach dem Meldegesetz 1991 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Meldewesens ist die Verarbeitung personenbezogener Daten von Meldepflichtigen in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Meldepflichtigen verbundenen Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des Meldewesens nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen, da das Melderegister sämtliche Personen mit Wohnsitz im Inland umfasst.

Überdies wäre im Falle der Geltendmachung des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung nicht mehr gewährleistet, dass das Melderegister, das aus Gründen der Publizität für die Öffentlichkeit in Bezug auf den Hauptwohnsitz als öffentliches Register geführt wird, Daten sämtlicher in Österreich wohnhafter Personen, enthält. Meldeauskünfte könnten demnach lediglich in eingeschränkter Weise erteilt werden. Dies würde den Zweck des Melderegisters – die Evidenthaltung der Meldedaten sämtlicher in Österreich wohnhafter Personen – vollständig konterkarieren. Die Evidenthaltung der Meldedaten ist für die gesamte staatliche Verwaltung von essentieller Bedeutung (siehe auch § 16a Abs. 4) sowie im Bereich des E-Government unerlässlich und vor allem für die Ermittlung der Kontaktdaten betroffener Personen, etwa für die Zustellung gerichtlicher und verwaltungsbehördlicher Dokumente (zB gesetzliche Zustellung von Urteilen und anderen Erledigungen, wie Ladungen), unverzichtbar. Zudem basiert die Wählerevidenz auf den Meldedaten (vgl. § 2 Abs. 1 Wählerevidenzgesetz 2018 – WEviG, BGBl. I Nr. 106/2016). Aus der ZMR-Zahl wird auch die Stammzahl natürlicher Personen und damit die Grundlage für den elektronischen Identitätsnachweis für E-Government-Zwecke abgeleitet. Eine geordnete, sparsame und effiziente Verwaltungsführung ist nicht möglich, wenn die Melderegister nicht mit dem Anspruch geführt werden, die richtigen Daten sämtlicher in Österreich niedergelassenen Personen zu erfassen. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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. Durch die gesetzlich normierten Datensicherheitsmaßnahmen sollen Missbrauch, unrechtmäßige Zugänge und unrechtmäßige Übermittlungen hintangehalten werden. 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 personenbezogenen Daten, 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 und 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 Meldebehörden 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 (zB auf der Homepage).

Die Möglichkeit, die Übermittlung der Meldedaten an Private zu beschränken (vgl. § 18 Abs. 2, Auskunftssperre), bleibt unabhängig davon bestehen. Damit existieren auch geeignete Vorkehrungen, um die Rechte und Freiheiten betroffener Personen zu schützen, die sich aus ihrer besonderen Situation ergeben.

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 des Meldewesens sowie die Funktionalität und die ordnungsgemäße Führung des Melderegisters gewährleisten.

Zu Art. 75 Z 20 bis 23 (§ 16a Abs. 1 bis 4 MeldeG):

Der geltende Abs. 1 kann zur Gänze entfallen, da sich die Berechtigung der Meldebehörden, die Daten des ZMR zu verarbeiten, bereits aus § 16 Abs. 1 ergibt.

In Abs. 2 soll die Klarstellung erfolgen, dass der Bundesminister für Inneres als Auftragsverarbeiter tätig wird.

Aufgrund der Änderungen im DSG ist es erforderlich, den Verweis in Abs. 3 an die neuen Regelungen anzupassen.

In Abs. 4 soll eine Verweisanpassung vorgenommen werden.

Zu Art. 75 Z 29 und 30 (§ 16b Abs. 3 und 4 MeldeG):

§ 4 Z 1 DSG 2000 definiert Daten dann als indirekt personenbezogen, wenn der Personenbezug derart ist, dass die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann. Diese Begriffsbestimmung findet sich weder in der DSGVO noch im Datenschutz-Anpassungsgesetz 2018, weshalb – wie in § 7 DSG („Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke“) – eine Klarstellung erfolgen soll, dass die Daten für statistische Zwecke an näher bestimmte Organe so zu übermitteln sind, dass sie für den Empfänger pseudonymisierte personenbezogene Daten sind (vgl. die Definition in Art. 4 Z 5 DSGVO) und der Empfänger (vgl. Art. 4 Z 9 DSGVO) die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Zudem soll in Abs. 4 eine Verweisanpassung an die neuen datenschutzrechtlichen Regelungen erfolgen.

Zu Art. 75 Z 31 (§ 16b Abs. 5 MeldeG):

Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken verarbeitet, so können bei Vorliegen näher bestimmter Voraussetzungen gemäß Art. 89 Abs. 2 DSGVO – vorbehaltlich der Bedingungen und Garantien gemäß Abs. 1 – durch nationales Recht Ausnahmen von den Rechten gemäß Art. 15 (Auskunftsrecht der betroffenen Person), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) vorgenommen werden. Da es in der Praxis kaum möglich wäre, gegenüber Betroffenen bei statistischen und wissenschaftlichen oder historischen Erhebungen aufgrund der Vielzahl, Vielfalt und des Umfangs der betroffenen personenbezogenen Daten sämtliche dieser Rechte zu wahren bzw. die Wahrung der Betroffenenrechte die Verwirklichung der spezifischen Forschungs- bzw. statistischen Zwecke ernsthaft beeinträchtigen, wenn nicht sogar unmöglich machen würde, soll die Ausnahmeermächtigung gemäß Art. 89 Abs. 2 DSGVO betreffend die im Zentralen Melderegister gespeicherten Daten in Anspruch genommen werden. Demzufolge soll, soweit personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken übermittelt werden, dem Betroffenen das

Recht auf Auskunft gemäß Art. 15 DSGVO nicht zukommen. Da bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke personenbezogene Daten, die nicht unter § 7 Abs. 1 DSG idF des Datenschutz-Anpassungsgesetzes 2018 fallen, nur dann verarbeitet werden dürfen, wenn dies entweder gesetzlich vorgesehen ist, eine Einwilligung der betroffenen Person erteilt wurde oder eine Genehmigung der Datenschutzbehörde vorliegt (vgl. § 7 Abs. 2 DSG), ist der Ausschluss dieses Rechts bei Übermittlungen jedenfalls gerechtfertigt und steht dieser – auch aufgrund der eingeschränkten Ausgestaltung – im Einklang mit den Vorgaben der DSGVO. Die weitere Verarbeitung der Daten zu den genannten Zwecken ist hingegen nicht Gegenstand dieser Bestimmung.

Zu Art. 75 Z 35 (§ 20 Abs. 3 MeldeG):

Es handelt es sich um eine redaktionelle Berichtigung.

Zu Art. 76 (Änderung des Passgesetzes 1992)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 4 B-VG („Passwesen“).

Zu Art. 76 Z 2 (§ 3 Abs. 5a des Passgesetzes 1992):

Die vorgeschlagene Änderung dient der Anpassung der für die Abnahme von Papillarlinienabdrücken geltenden Voraussetzungen an die Vorgaben der DSGVO.

Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 DSG 2000. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Im gegebenen Zusammenhang ist der Tatbestand des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Datenverarbeitung der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen muss. Der Zweck für die Abnahme von Papillarlinienabdrücken liegt in der Erfüllung einer unionsrechtlichen Verpflichtung in Bezug auf die Sicherung der Identitätsfeststellung (EuGH vom 17.10.2013, Rs C-291/12, *Schwarz* gegen *Bochum*; vgl. auch Verordnung [EG] Nr. 444/2009 zur Änderung der Verordnung [EG] Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. Nr. L 142 vom 28.05.2009 S. 1, wonach die Mitgliedstaaten auch für angemessene Verfahren zur Wahrung der Würde der betroffenen Person zu sorgen und die Menschenrechte zu wahren haben sowie Altersgrenzen vorgesehen sind).

In den Fällen des – hier einschlägigen – Art. 9 Abs. 2 lit. g DSGVO sind „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ gesetzlich vorzusehen. Diesem Erfordernis wird durch Rechnung getragen, dass vorgeschlagen wird, die Abnahme von Papillarlinienabdrücken ausschließlich geeigneten und besonders geschulten Bediensteten der Passbehörde bzw. den Bürgermeistern (vgl. § 16 Abs. 3) vorzubehalten. Handelt es sich bei diesen Personen um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder den §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Abnahme von Papillarlinienabdrücken durch Personen, für die weder die Vorschriften des BDG noch des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Abnahme von Papillarlinienabdrücken – etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung – zur Verschwiegenheit verpflichtet sind. Weiters wird die Abnahme von Papillarlinienabdrücken – nach dem bewährten Vorbild des § 13 FPG – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Zu Art. 76 Z 3, 4, 7, 8, 10, 11 und 12 (§ 3 Abs. 6 und 9, § 16 Abs. 3 und 6, § 17 Abs. 2, Überschrift zu § 22a, § 22a Abs. 1, 3 und 4, Überschrift zu § 22b, § 22b Abs. 2 und 3, § 22d Abs. 2 des Passgesetzes 1992):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im Passgesetz 1992 verwendeten Begriffe erforderlich erscheint, sollen diese an die Definitionen der DSGVO (Art. 4 DSGVO) angeglichen werden. Beispielsweise sollen die Begriffe „überlassen“, „zur Verfügung stellen“, das „Weitergeben“ oder das „Weiterleiten“ von Daten durch „übermitteln“ ersetzt werden.

Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der „Auftragsverarbeiter“

(§ 4 Z 8 DSGVO) deckt sich mit dem bisherigen „Dienstleister“ im Sinne des DSG 2000. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Zu Art. 76 Z 6 (§ 3 Abs. 8 des Passgesetzes 1992):

Es handelt sich um eine Verweis- sowie eine Begriffsanpassung an die neuen datenschutzrechtlichen Regelungen der DSGVO.

Zu Art. 76 Z 7 (§ 16 Abs. 3 des Passgesetzes 1992):

Es handelt sich um die Bereinigung eines legistischen Versehens.

Zu Art. 76 Z 8 (§ 16 Abs. 6 des Passgesetzes 1992):

Die Bundesrechenzentrum GmbH nimmt bereits nach derzeitiger Rechtslage die Rechten und Pflichten eines Dienstleisters im Sinne des § 4 Z 5 DSG 2000 wahr, weshalb die Bezeichnung der Bundesrechenzentrum GmbH als Auftragsverarbeiterin nur eine klarstellende Funktion hat. Zudem soll ausdrücklich gesetzlich normiert werden, dass sie als Auftragsverarbeiterin auch zur Einhaltung der Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO verpflichtet ist.

Zu Art. 76 Z 9 und Z 17 (§ 17 Abs. 2, § 22b Abs. 3 und 4, § 22c Abs. 4 und § 22d Abs. 2 des Passgesetzes 1992):

Es soll im Sinne der neuen datenschutzrechtlichen Terminologie klargestellt werden, dass es sich bei diesen Daten um personenbezogene Daten handelt.

Zu Art. 76 Z 13 (§ 22a Abs. 6 des Passgesetzes 1992):

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, im Rahmen der lokalen Anwendungen und der zentralen Evidenz in § 22a Abs. 6 und § 22b Abs. 5 eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Zu Art. 76 Z 14 und 15 (§ 22b Abs. 1 bis 1b des Passgesetzes 1992):

Im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie das in der DSGVO normierte Transparenzgebot (vgl. ErwGr 60 zur DSGVO; siehe auch Art. 5 DSGVO), soll im Einleitungsteil des Abs. 1 der Zweck der Datenverarbeitung festgelegt werden.

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Art. 26 DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 22b entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der Zentralen Evidenz verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 1a die Zuständigkeit zwischen den gemeinsam Verantwortlichen der zentralen Evidenz dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll nach Abs. 1a direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier (Abs. 1a) – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf die zentrale Evidenz bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig durch Abs. 1b die Funktion des Auftragsverarbeiters zu übertragen. Zudem soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen sowie – vergleichbar den Regelungen in anderen Materiengesetzen (vgl. § 44 Abs. 3 PStG 2013, § 16 Abs. 7 MeldeG, § 56a Abs. 2 StbG) – datenqualitätssichernde Maßnahmen zu setzen, wie insbesondere Hinweise auf eine mögliche Identität zweier ähnlicher Datensätze oder die Schreibweise von Adressen zu geben („Clearing“). Zu einer Korrektur der Daten durch den Bundesminister für Inneres kommt es hingegen nicht. Darüber hinaus darf der Bundesminister für Inneres wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Art. 76 Z 18 (§ 22b Abs. 6 des Passgesetzes 1992):

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 § 22b Abs. 6 für sämtliche nach dem Passgesetz 1992 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Passwesens ist die Verarbeitung personenbezogener Daten von Antragstellern eines Reisedokuments in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen

werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten Betroffener verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (siehe auch Art. 23 Abs. 1 lit. h DSGVO) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich.

Die Datenverarbeitung in der zentralen Evidenz ist Grundvoraussetzung für die Ausstellung eines Reisepasses oder Personalausweises. Im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung wäre die Besorgung der Aufgaben nach diesem Bundesgesetz und ein geordneter, sparsamer und effizienter Vollzug des Passwesens nicht mehr möglich.

Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen, da die zentrale Evidenz und die lokalen Anwendungen sämtliche Personen, die bei der Behörde ein Reisedokument beantragt haben, umfassen. Überdies können Behörden durch den Rückgriff auf frühere Dokumente und Daten die Identität des Antragstellers gesichert feststellen und insbesondere mittels Vergleich mit früheren Lichtbildern ein Erschleichen von Dokumenten und somit Missbrauch verhindern (zB Erschleichung eines Dokuments auf den Namen einer anderen Person unter Vorlage des eigenen Lichtbilds). Die Verarbeitung der Daten bringt zudem eine Erleichterung für die Bürger, da es nicht mehr erforderlich ist, bei Beantragung eines neuen Reisepasses oder Personalausweises sämtliche Dokumente erneut vorzulegen. Darüber hinaus liegt der Verarbeitung von bestimmten Daten (so zB von Papillarlinienabdrücken sowie Lichtbildern) eine unionsrechtliche Verpflichtung zugrunde. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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 personenbezogenen Daten, 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 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 Passbehörden 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 (zB auf der 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 des Passwesens sowie die Funktionalität und die ordnungsgemäße Führung der zentralen Evidenz gewährleisten.

Zu Art. 76 Z 19 (§ 22d Abs. 2 des Passgesetzes 1992):

Es handelt sich um Anpassungen an die aktuelle europarechtliche Terminologie.

Zu Art. 77 (Änderung des Personenstandsgesetzes 2013)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Personenstandsangelegenheiten einschließlich des Matrikenwesens und der Namensänderung“).

Zu Art. 77 Z 3, 4, 5, 7, 9, 11, 15, 17, 19, 22, 23, 26, 27, 32, 39, 41 und 45 (§ 7 Abs. 3, § 8, § 9 Abs. 1, 5 und 6, § 12, § 28 Abs. 1 und 5, § 31, § 41 Abs. 3, § 43 Abs. 1, § 45 Abs. 3, Überschrift zum 4. Hauptstück, Überschrift zum 1. Abschnitt des 4. Hauptstückes, § 46 Abs. 4, § 47 Abs. 1 und 4, § 48 Abs. 4, § 50, § 52 Abs. 4, § 61 Abs. 1, 5 und 6 PStG 2013):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im Personenstandsgesetz 2013 verwendeten Begriffe erforderlich erscheint, werden diese nun an die Definitionen der DSGVO (Art. 4 DSGVO) angeglichen. Beispielsweise sollen die Begriffe „mitteilen“, „überlassen“, „zur Verfügung stellen“, das „Weitergeben“ oder das „Weiterleiten“ von Daten durch „übermitteln“ ersetzt werden.

Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der „Auftragsverarbeiter“ (§ 4 Z 8 DSGVO) deckt sich mit dem bisherigen „Dienstleister“ im Sinne des DSG 2000. Soweit es sich hingegen bei der Datenanwendung um ein Informationsverbundsystem handelt, entspricht der Auftragsverarbeiter im Sinne der DSGVO dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Personenstandsregister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Soweit Personenstandsbehörden personenbezogene Daten im Wege eines Änderungszugriffes an das Zentrale Melderegister übermitteln, wie dies in §§ 12 und 31 vorgesehen ist, sollen diese für die Meldebehörden als Auftragsverarbeiter tätig werden.

Zu Art. 77 Z 6 (§ 9 Abs. 5, § 46 Abs. 3, § 58 Abs. 1, § 61 Abs. 2 PStG 2013):

Soweit der Begriff „Daten“ durch „personenbezogene Daten“ ersetzt wurde, bewirkt diese vorgeschlagene Ergänzung keine inhaltliche Änderung. Vielmehr handelt es sich um eine Klarstellung.

Zu Art. 77 Z 8 und 14 (§ 9 Abs. 5, § 28 Abs. 5 PStG 2013):

Im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie das in der DSGVO normierte Transparenzgebot (vgl. ErwGr 60 zur DSGVO; siehe auch Art. 5 DSGVO), soll der konkrete Zweck der Datenverarbeitung in § 9 Abs. 5 sowie § 28 Abs. 5 festgelegt werden.

Mittels der vorgeschlagenen Änderung soll demnach klargestellt werden, dass der Bundesanstalt Statistik Österreich die Daten gemäß § 8 Abs. 1 des Hebammengesetzes, BGBl. Nr. 310/1994, und die Daten zur Todesursache, die Vornahme einer Obduktion sowie Angaben zur Müttersterblichkeit im Wege des ZPR bloß zu statistischen Zwecken übermittelt werden dürfen.

Zu Art. 77 Z 10 und 12 (§ 11 Abs. 4, § 20 Abs. 5, § 27 Abs. 4 PStG 2013):

Die Angabe des Religionsbekenntnisses anlässlich der Eintragung der Geburt, der Ehe oder der Eingetragenen Partnerschaft ist bereits nach geltendem Recht nicht obligatorisch. Durch die Änderung dieser Bestimmung wird dies nun ausdrücklich klargestellt.

Zu Art. 77 Z 16 (§ 42 Abs. 3 PStG 2013):

Aufgrund der Tatsache, dass sich das Recht des Betroffenen auf Berichtigung aus Art. 16 DSGVO ergibt, soll die sich direkt aus dem PStG 2013 ergebende Möglichkeit, auf Antrag eine Berichtigung zu verlangen, in Abs. 3 entfallen, ohne dass dies eine Beschränkung der Betroffenenrechte zur Folge hat.

Zu Art. 77 Z 18 (§ 44 samt Überschrift PStG 2013):

Zu Abs. 1:

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO (siehe die Erläuterungen zu den begrifflichen Anpassungen). Art. 26 DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 44 entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der im Zentralen Personenstandsregister (ZPR) verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Zu Abs. 1a:

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 1a die Zuständigkeit zwischen den gemeinsam Verantwortlichen des ZPR dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier (Abs. 1a) – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Zu Abs. 2:

Vor dem Hintergrund des Entfalls von § 17 Abs. 2 DSG 2000, wonach gemäß Z 1 Datenanwendungen, die die Führung von öffentlichen Registern zum Inhalt haben, nicht meldepflichtig sind, ist die Klarstellung, dass es sich beim Zentralen Personenstandsregister um ein öffentliches Register handelt, nicht mehr erforderlich.

Zu Abs. 3:

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Personenstandsregister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Zudem soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 5:

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, im Rahmen des ZPR eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Zu Abs. 6:

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 § 44 Abs. 6 für sämtliche nach dem Personenstandsgesetz 2013 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Personenstandswesens ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Betroffenen verbundenen Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des Personenstandswesens nicht mehr möglich.

Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen, da das Personenstandsregister Daten zu sämtlichen Personenstandsfällen umfasst. Überdies wäre im Falle der Geltendmachung des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung nicht mehr gewährleistet, dass das Personenstandsregister, das aus Gründen der Publizität für die Öffentlichkeit in Bezug auf die Daten zum Tod einer Person als öffentliches Register geführt wird, Daten sämtlicher Personenstandsfälle enthält. Dies hätte zur Folge, dass Auskunftserteilungen aus dem

Personenstandsregister lediglich in eingeschränkter Weise erteilt werden könnten. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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. Durch die gesetzlich normierten Datensicherheitsmaßnahmen sollen Missbrauch, unrechtmäßige Zugänge und unrechtmäßige Übermittlungen hintangehalten werden. 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 personenbezogenen Daten, 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 Personenstandsbehörden 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 (zB auf der 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 des Personenstandswesens sowie die Funktionalität und die ordnungsgemäße Führung des Personenstandsregisters gewährleisten.

Zu Art. 77 Z 20 und 21 (§ 45 Abs. 3 und 4 PStG 2013):

§ 4 Z 1 DSG 2000 definiert Daten dann als indirekt personenbezogen, wenn der Personenbezug derart ist, dass die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann. Diese Definition findet sich weder in der DSGVO noch im Datenschutz-Anpassungsgesetz 2018, weshalb – wie in § 7 DSG („Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke“) – in Abs. 3 eine Klarstellung erfolgen soll, dass die Daten für statistische Zwecke an näher bestimmte Organe so zu übermitteln sind, dass sie für den Empfänger pseudonymisierte personenbezogene Daten sind (vgl. die Definition in Art. 4 Z 5 DSGVO) und der Empfänger (vgl. Art. 4 Z 9 DSGVO) die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Betreffend die vorgeschlagenen Ergänzungen in Abs. 4 wird auf die Erläuterungen zu § 44 Abs. 5 verwiesen.

Zu Art. 77 Z 24 (§ 46 Abs. 1 und 2 PStG 2013):

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO entspricht dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Vor diesem Hintergrund ergibt sich die Berechtigung der Personenstandsbehörden, die im ZPR verarbeiteten Daten zu verwenden, bereits aus § 44 Abs. 1, weshalb diese Passagen in Abs. 1 und 2 entfallen können.

Zu Art. 77 Z 28 bis 30, 35 bis 38 (Überschrift zu § 48, § 48 Abs. 1 bis 3, 5, 7 bis 12, § 49, § 51 Abs. 1 PStG 2013):

Da sich aus der DSGVO ergibt, dass der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen sollte (ErwGr 15 zur DSGVO), wird künftig von der begrifflichen Differenzierung zwischen „zur Verfügung stellen“ und „übermitteln“ Abstand genommen (siehe auch die Erläuterungen zu den terminologischen Anpassungen).

Im vorgeschlagenen Abs. 12 soll lediglich eine Anpassung an die neue Systematik erfolgen.

Zu Art. 77 Z 33 (§ 48 Abs. 4a PStG 2013):

Mit der vorgeschlagenen Änderung wird einem Wunsch aus der Praxis nachgekommen. Es ist von enormer Bedeutung, dass der Datenbestand im Strafregister aktuell gehalten wird, da andererseits aufgrund von Namensänderungen die Gefahr besteht, dass unrichtige bzw. unvollständige Strafregisterbescheinigungen ausgestellt werden. Daher sollen die Daten zu allen Namensänderungen von strafmündigen Personen sowie zum Tod einer Person auch dem Strafregisteramt der Landespolizeidirektion Wien im Wege des Bundesministers für Inneres als Auftragsverarbeiter gemäß § 1 Abs. 3 Strafregistergesetz 1968 übermittelt werden. Einer Aktualisierung der Daten bedarf es selbstverständlich nur in jenen Fällen, in denen die geänderten Daten des jeweiligen Betroffenen bereits im Strafregister verarbeitet wurden.

Zu Art. 77 Z 39 (§ 50 PStG 2013):

Die Daten zum Tod einer Person können im Rahmen des Änderungsdienstes auf Verlangen gegen Kostenersatz übermittelt werden. Eine Änderung der Daten zum Tod einer Person wäre jedoch denkunmöglich und soll vor diesem Hintergrund entfallen.

Zu Art. 77 Z 41 und 42 (§ 52 Abs. 4 und 4a PStG 2013):

In Abs. 4 erfolgt die Verweisanpassung an das neue DSG idFd Datenschutz-Anpassungsgesetzes 2018 sowie die Bereinigung eines redaktionellen Versehens. Soweit personenbezogene Daten von mehr als einem Auftraggeber zu übermitteln sind, kommt diese Aufgabe dem Bundesminister für Inneres als Auftragsverarbeiter zu. Dabei handelt es sich um eine durch Gesetz übertragene Verpflichtung ohne Ermessen; der Bundesminister für Inneres ist zudem nicht befugt, über die Zwecke und Mittel der Verarbeitung zu entscheiden.

Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, so können bei Vorliegen näher bestimmter Voraussetzungen gemäß Art. 89 Abs. 2 DSGVO – vorbehaltlich der Bedingungen und Garantien gemäß Abs. 1 – durch nationales Recht Ausnahmen von den Rechten gemäß Art. 15 (Auskunftsrecht der betroffenen Person), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) vorgenommen werden. Da es in der Praxis kaum möglich wäre, gegenüber Betroffenen bei statistischen und wissenschaftlichen Erhebungen aufgrund der Vielzahl, Vielfalt und des Umfangs der betroffenen personenbezogenen Daten sämtliche dieser Rechte zu wahren bzw. die Wahrung der Betroffenenrechte die Verwirklichung der spezifischen Forschungs- bzw. statistischen Zwecke ernsthaft beeinträchtigen, wenn nicht sogar unmöglich machen würde, soll die Ausnahmeermächtigung gemäß Art. 89 Abs. 2 DSGVO betreffend die im Zentralen Personenstandsregister gespeicherten Daten in Anspruch genommen werden. Demzufolge soll, soweit personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken übermittelt werden, dem Betroffenen das Recht auf Auskunft gemäß Art. 15 DSGVO nicht zukommen. Da bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke personenbezogene Daten, die nicht unter § 7 Abs. 1 DSG idF des Datenschutz-Anpassungsgesetzes 2018 fallen, nur dann verarbeitet werden dürfen, wenn dies entweder gesetzlich vorgesehen ist, eine Einwilligung der betroffenen Person erteilt wurde oder eine Genehmigung der Datenschutzbehörde vorliegt (vgl. § 7 Abs. 2 DSG), ist der Ausschluss dieses Rechts bei Übermittlungen jedenfalls gerechtfertigt und steht dieser – auch aufgrund der eingeschränkten Ausgestaltung – im Einklang mit den Vorgaben der DSGVO. Die weitere Verarbeitung der Daten zu den genannten Zwecken ist hingegen nicht Gegenstand dieser Bestimmung.

Zu Art. 77 Z 43 (§ 52 Abs. 5 Z 3 PStG 2013):

Es handelt sich um die Bereinigung eines redaktionellen Versehens.

Zu Art. 77 Z 44 (§ 53 Abs. 7, § 58 Abs. 2 PStG 2013):

Es soll die Klarstellung erfolgen, dass es sich um die Amtssignatur des Bundesministers für Inneres handelt.

Zu Art. 77 Z 47 (§ 61 Abs. 7 PStG 2013):

Aufgrund der zeitlich eingeschränkten Möglichkeit, bis 1. Juni 2015 eine Verordnung zu erlassen, kann diese Verordnungsermächtigung mangels Anwendungsbereich entfallen.

Zu Art. 77 Z 48 und 49 (§ 72 Abs. 3 bis 8 PStG 2013):

Die rechtliche Grundlage für den Testbetrieb des ZPR in Abs. 3 kann vor dem Hintergrund der bereits erfolgten Aufnahme des Echtbetriebs am 1. November 2014 entfallen. Zwecks besserer Lesbarkeit soll eine Neunummerierung der bisherigen Abs. 4 bis 9 erfolgen.

Zu Art. 78 (Änderung des Pyrotechnikgesetzes 2010)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Waffen-, Munitions- und Sprengmittelwesen, Schießwesen“).

Zu Art. 78 Z 1 und 2 (§ 10 Abs. 1, 3 und 4):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der „Auftragsverarbeiter“ (§ 4 Z 8 DSGVO) deckt sich mit dem bisherigen „Dienstleister“ im Sinne des DSG 2000. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Soweit der Begriff „Daten“ durch „personenbezogene Daten“ ersetzt wurde, bewirkt diese vorgeschlagene Ergänzung keine inhaltliche Änderung. Vielmehr handelt es sich um eine Klarstellung.

Darüber hinaus wurden Verweisanpassungen vorgenommen.

Zu Art. 78 Z 3 (§ 19 Abs. 4):

Betreffend das Verhältnis zwischen Bundesminister für Inneres und dem gemeinsamen Auftragsverarbeiter orientieren sich die vorgeschlagenen Änderungen an der Regelung in § 3 Abs. 6 und 8 Passgesetz 1992 und haben – ohne eine Änderung der tatsächlichen Vollzugspraxis herbeizuführen – lediglich eine klarstellende Funktion.

Im Hinblick auf die terminologischen Anpassungen wird auf die Erläuterungen zu § 10 verwiesen.

Zu Art. 79 (Änderung des Vereinsgesetzes 2002)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Vereins- und Versammlungsrecht“).

Zu Art. 79 Z 4, 5, 8, 13,18 bis 20 (Überschrift zum 3. Abschnitt, Überschrift zu § 15, § 15, § 16 Abs. 1 und 5, § 17 Abs. 4, § 19 Abs. 4 bis 6 VerG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im Vereinsgesetz 2002 verwendeten Begriffe erforderlich erscheint, werden diese nun an die Definitionen der DSGVO (Art. 4 DSGVO) angeglichen. Beispielsweise sollen die Begriffe „verwenden“ und „evident halten“ durch „verarbeiten“, „zur Verfügung stellen“ durch „übermitteln“ sowie „Datenanwendungen“ durch „Datenverarbeitungen“ ersetzt werden.

Zudem soll im Hinblick auf die neuen Begrifflichkeiten die Wortfolge „sensible Daten“ auf „besondere Kategorie personenbezogener Daten“ (vgl. Art. 9 DSGVO) angepasst werden.

Zu Art. 79 Z 4 (§ 15 VerG):

Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 DSG 2000. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Im gegebenen Zusammenhang ist der Tatbestand des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Datenverarbeitung der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen muss. Dies vor dem Hintergrund, dass die Vereinsbehörden ihrer gesetzlich vorgesehenen Informations- und Prüfpflicht nur dann nachkommen können, wenn sie die erforderlichen

Vereinsdaten zweckgemäß verarbeiten können. Anknüpfungspunkt für besondere Kategorien personenbezogener Daten ist dabei der Vereinsname, der gemäß § 4 Abs. 1 einen Schluss auf den Vereinszweck zulassen muss. Dies kann zur Folge haben, dass zB ein auf eine bestimmte ethnische Herkunft oder politische Überzeugung hindeutender Name eines Vereins einen Rückschluss auf die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit der Vereinsorgane mit sich bringt.

In den Fällen des – hier einschlägigen – Art. 9 Abs. 2 lit. g DSGVO sind „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" gesetzlich vorzusehen. Diesem Erfordernis wird durch Festlegung angemessener Schutzgarantien zugunsten besonderer Kategorien personenbezogener Daten in Form einer Differenzierung nach Datenarten und „Auskunftsebenen" (§ 17 Abs. 1 und Abs. 2, § 19 Abs. 2 und Abs. 3) sowie in Gestalt einer Auskunftssperre (§ 17 Abs. 4 bis 6) Rechnung getragen.

Zu Art. 79 Z 5, 7 und 8 (§ 16 Abs. 1, 4 und 5 VerG):

Im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie das in der DSGVO normierte Transparenzgebot (vgl. ErwGr 60 zur DSGVO; siehe auch Art. 5 DSGVO), soll in Abs. 1 der Zweck der Datenverarbeitung festgelegt werden.

Aufgrund der Tatsache, dass sich das Recht des Betroffenen auf Berichtigung aus Art. 16 DSGVO ergibt, soll die sich direkt aus dem Vereinsgesetz 2002 ergebende Möglichkeit, auf Antrag eine Berichtigung zu verlangen, in Abs. 4 entfallen, ohne dass dies eine Beschränkung der Betroffenenrechte zur Folge hat.

In Abs. 5 erfolgt zudem die Beseitigung eines redaktionellen Versehens.

Zu Art. 79 Z 6, 11, 17 und 22 (§ 16 Abs. 1 Z 3, § 17 Abs. 1 Z 1, § 19 Abs. 2 und § 31 Z 4 lit. e VerG):

Es handelt sich um Verweisanpassungen.

Zu Art. 79 Z 9 (§ 16 Abs. 6 VerG):

§ 14 DSG 2000 sieht 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. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. 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 bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden.

Zu Art. 79 Z 10 (Überschrift zu § 17 VerG):

Es handelt sich um eine Anpassung der Überschrift an die Regelung in § 17.

Zu Art. 79 Z 11 und 12 (§ 17 Abs. 1 und 2 VerG):

Vor dem Hintergrund des Entfalls von § 17 Abs. 2 DSG 2000, wonach gemäß Z 1 Datenanwendungen, die die Führung von öffentlichen Registern zum Inhalt haben, nicht meldepflichtig sind, ist die Klarstellung in Abs. 1, dass es sich beim Lokalen Vereinsregister um ein öffentliches Register handelt, nicht mehr erforderlich.

Im Hinblick auf die Änderungen des DSG 2000 aufgrund des Datenschutz-Anpassungsgesetzes 2018, kann der Verweis auf das DSG 2000 in Abs. 2 entfallen.

Zu Art. 79 Z 15 (§ 18 VerG):

Zu Abs. 1:

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt.

Art. 26 DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 18 entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der im Zentralen Vereinsregister (ZVR) verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung

gestellt hat – offensteht, ist damit nicht verbunden. Zudem sollen wie bisher die Vereinsbehörden verpflichtet sein, dem Bundesminister für Inneres für die Zwecke der Führung des ZVR unverzüglich ihre Vereinsdaten gemäß § 16 Abs. 1 Z 1 bis 17 im Wege der Datenfernübertragung zu übermitteln.

Zu Abs. 1a:

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 1a die Zuständigkeit zwischen den gemeinsam Verantwortlichen des ZVR dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Informations-, Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten nach der DSGVO treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier (Abs. 1a) – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Zu Abs. 1b:

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das ZVR bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Zudem soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 2:

Es handelt sich lediglich um eine Klarstellung.

Zu Abs. 3:

Betreffend die Protokollierungsregelungen wird auf § 16 Abs. 6 verwiesen.

Zu Abs. 4:

Da sich der Verweis auf § 17 Abs. 1 hinsichtlich der Auskünfte aus dem Lokalen Vereinsregister bereits aus dem vorgeschlagenen § 19 Abs. 1 ergibt, kann der geltende § 18 Abs. 4 entfallen.

Ab Inkrafttreten der DSGVO hat der Betroffene gemäß Art. 21 Abs. 1 DSGVO 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 § 18 Abs. 4 für sämtliche nach dem Vereinsgesetz 2002 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Vereinswesens ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung als allgemeines öffentliches Interesse, zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Betroffenen verbundenen Ordnungsfunktion sowie zum Schutz wichtiger Ziele des allgemeinen öffentliches Interesses (zB zur Abklärung steuerrechtlicher und zivilrechtlicher Fragestellungen) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des Vereinswesens nicht mehr möglich.

Überdies wäre im Falle der Geltendmachung des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung nicht mehr gewährleistet, dass das Vereinsregister, das aus Gründen der Publizität für die Öffentlichkeit in Bezug auf Daten gemäß § 16 Abs. 1 Z 1 bis 7, 10 bis 13 und 16 als öffentliches Register geführt wird, Daten sämtlicher Vereinsorgane, die unter anderem zur Vertretung des Vereins nach außen befugt sind, enthält. Dies hätte zur Folge, dass Auskunftserteilungen aus dem Vereinsregister lediglich in eingeschränkter Weise erteilt werden könnten und dies den Rechtsverkehr erheblich erschweren würde. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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. Durch die gesetzlich normierten Datensicherheitsmaßnahmen sollen Missbrauch, unrechtmäßige Zugänge und unrechtmäßige Übermittlungen hintangehalten werden. 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 personenbezogenen Daten, 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 Vereinsbehörden 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 (zB auf der 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 des Vereinswesens sowie der Funktionalität und die ordnungsgemäße Führung des Vereinsregisters gewährleisten.

Zu Art. 79 Z 16, 17 und 21 (Überschrift zu § 19, § 19 Abs. 1, 3 und 7 VerG):

Die Überschrift soll an die neuen Regelungen in § 19 angepasst werden.

Da sich die Möglichkeit der Vereinsbehörden, personenbezogene Daten des Zentralen Vereinsregisters zu verarbeiten, bereits aus dem vorgeschlagenen § 18 ergibt, kann § 19 Abs. 1 erster Satz entfallen.

Betreffend den Entfall des Begriffs „öffentliches Register“ in Abs. 3, wird auf die Erläuterungen zu § 17 verwiesen.

Nach dem geltenden § 19 Abs. 3 ist eine Online-Einzelabfrage nur nach den in § 17 Abs. 1 Z 1 bis 3 näher normierten Suchkriterien sowie für die in § 16 Abs. 1 Z 1 bis 7, 10 bis 13 und 16 angeführten Daten vorgesehen, wie sich aus der Einschränkung „[i]nsoweit das ZVR ein öffentliches Register ist (§ 17 Abs. 1)“ ergibt. Da keine Ausdehnung der erfassten Datenkategorien intendiert ist und zudem weiterhin nur eine Abfrage eines nach § 17 Abs. 1 Z 1 bis 3 eindeutig bestimmbaren Vereins möglich sein soll, sollen entsprechende Verweise eingefügt werden.

Mit der vorgeschlagenen Änderung in Abs. 7 wird einem Wunsch aus der Praxis nachgekommen. Im Hinblick auf die der Österreichischen Nationalbank gesetzlich oder gemeinschaftsrechtlich zugewiesenen Aufgaben soll der Österreichischen Nationalbank der Zugang zu Daten des Vereinsregisters über eine automatisierte Schnittstelle eingeräumt werden. Die Verordnung (EU) 2016/867 über die Erhebung granularer Kreditdaten und Kreditrisikodaten (EZB/2016/13), ABl. Nr. L 144 vom 18.5.2016 S. 44, („AnaCredit-Verordnung“), die seit 31. Dezember 2017 gilt, sieht vor, dass beginnend mit 30. September 2018 Kreditaufnahmen von Firmen und sonstigen juristischen Personen bereits ab einer Höhe von 25 000 Euro – und nicht mehr wie bisher ab 350 000 Euro – an die Österreichische Nationalbank zu melden sind. Da durch die deutliche Senkung der Meldegrenze mit einer Vervielfachung der meldepflichtigen Vereine und somit mit einem enorm steigenden Verwaltungsaufwand zu rechnen ist, ist im Sinne der Verwaltungsökonomie beabsichtigt, eine Automatisierung der Prozesse einzuführen. Angelehnt an die bewährte Vorgehensweise bei im Firmenbuch protokollierten Unternehmen (vgl. § 22 Abs. 2a Firmenbuchgesetz, BGBl. Nr. 10/1991) soll eine tägliche Datenübermittlung aus dem Vereinsregister implementiert werden. Dies soll einerseits sowohl bei der österreichischen Kreditwirtschaft als auch bei der Österreichischen Nationalbank zu einer Reduzierung des Aufwands betreffend Neuanmeldungen und Änderungsmeldungen zu Stammdaten von Vereinen führen und andererseits eine Verbesserung der Datenbasis und Datenqualität zur Folge haben.

Zu Art. 79 Z 22 (§ 31 Z 4 lit. e VerG):

Es handelt sich um eine sprachliche Anpassung an § 18 Abs. 2.

Zu Art. 80 (Änderung des Waffengesetzes 1996)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Waffen-, Munitions- und Sprengmittelwesen, Schießwesen“).

Zu Art. 80 Z 2 (§ 21 Abs. 5 und 6 WaffG):

Die Eintragung der Registernummer des Auftraggebers ergibt sich nach geltender Rechtslage aus § 25 DSG 2000, wonach bei meldepflichtigen Datenanwendungen die Pflicht zur Offenlegung der Identität des Auftraggebers auch die Registernummer umfasst. Da die Meldepflichten an die Datenschutzbehörde mit Inkrafttreten des Datenschutz-Anpassungsgesetzes 2018 wegfallen und somit künftig auch keine Registrierung eines Verantwortlichen bei dieser Behörde vorzunehmen ist, kann in Abs. 5 die Anführung der Registernummer auf Waffenbesitzkarten und Waffenpässen entfallen.

Betreffend das Verhältnis zwischen dem Bundesminister für Inneres und dem gemeinsamen Auftragsverarbeiter orientieren sich die vorgeschlagenen Änderungen in Abs. 6 an § 3 Abs. 6 und 8 Passgesetz 1992 und haben – ohne eine Änderung der tatsächlichen Vollzugspraxis herbeizuführen – lediglich eine klarstellende Funktion.

Zu Art. 80 Z 2, 3, 4, 13, 14, 15 und 17 (§ 21 Abs. 5 und 6, Überschrift zum 11. Abschnitt, § 54 Abs. 1, § 55 Abs. 6 bis 9 WaffG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ (Art. 4 Z 7 DSGVO) einer Datenverarbeitung. Der „Auftragsverarbeiter“ (§ 4 Z 8 DSGVO) deckt sich mit dem bisherigen „Dienstleister“ im Sinne des DSG 2000. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Soweit der Begriff „Daten“ durch „personenbezogene Daten“ ersetzt wurde, bewirkt diese vorgeschlagene Ergänzung keine inhaltliche Änderung. Vielmehr handelt es sich um eine Klarstellung.

Zu Art. 80 Z 6 (§ 54 Abs. 2 WaffG):

In Abs. 2 wird eine terminologische Anpassung vorgenommen, da in der DSGVO (Art. 4 Z 10) „Dritten“ eine andere Bedeutung zugrunde gelegt wird. Dadurch soll sich jedoch keine inhaltliche Änderung im Vergleich zur geltenden Rechtslage ergeben.

Zu Art. 80 Z 7 (§ 54 Abs. 2a WaffG):

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 § 54 Abs. 2a für sämtliche nach dem Waffengesetz 1996 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Waffenwesens ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass

ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Personen mit registrierten Schusswaffen sowie Inhabern von waffenrechtlichen Dokumenten verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (siehe auch Art. 23 Abs. 1 lit. h DSGVO) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des Waffenwesens nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen, da die Zentrale Informationssammlung sämtliche Personen mit registrierten und bewilligten Schusswaffen umfasst.

Dies würde im Anwendungsbereich des Waffenregisters dazu führen, dass der unionsrechtlichen Verpflichtung zur Führung eines elektronischen Waffenregisters, in das die Feuer- bzw. Schusswaffen eingetragen werden, nicht nachgekommen werden könnte (vgl. Richtlinie [EU] 2008/51 zur Änderung der Richtlinie 91/477/EWG des Rates über die Kontrolle des Erwerbs und des Besitzes von Waffen, ABl. Nr. L 179 vom 8.7.2008 S. 5). Überdies wäre im Falle der Geltendmachung des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung nicht mehr gewährleistet, dass sämtliche registrierungs- und bewilligungspflichtigen Waffen, Inhaber waffenrechtlicher Dokumente sowie Waffenverbote in der Zentralen Informationssammlung enthalten sind, was aus Gründen der öffentlichen Sicherheit bedenklich wäre. Betroffene, über die ein Waffenverbot gemäß § 12 f verhängt wurde, könnten etwa ohne weiteres wieder in den Besitz von Schusswaffen der Kategorie C kommen, da bei Geltendmachung des Rechts auf Widerspruch bzw. Einschränkung der Verarbeitung Waffenverbote in der Zentralen Informationssammlung nicht ersichtlich wären. Aus diesem Grund bestünde auch keine Möglichkeit, dass Organe des öffentlichen Sicherheitsdienstes Waffen oder Munition sicherstellen. Darüber hinaus könnten Waffenverbote, sofern eine gesetzliche Grundlage für die Übermittlung von bestehenden Waffenverboten geschaffen wurde, bei Eignungsfeststellungen (zB im Falle einer Bewerbung als Kindergartenpädagoge) nicht als Entscheidungsgrundlage dienen. Weiters wäre nicht mehr gewährleistet, dass Gerichte und sonstige Behörden sämtliche Daten und Informationen, die diese für eine rechtsrichtige Entscheidung benötigen, tatsächlich heranziehen können und könnte dies – vor allem bei Gefahr im Verzug (Gewalt in der Familie, Gefährderprognosen etc.) – in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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. Durch die gesetzlich normierten Datensicherheitsmaßnahmen sollen Missbrauch, unrechtmäßige Zugänge und unrechtmäßige Übermittlungen hintangehalten werden. 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 personenbezogenen Daten, 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 Verantwortlichen 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 (zB auf der 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 des Waffengesetzes sowie die Funktionalität und die ordnungsgemäße Führung des Waffenregisters gewährleisten.

Zu Art. 80 Z 8 (§ 54 Abs. 3 WaffG):

Die Mitwirkung der Bundesrechenzentrum GmbH wird in Abs. 3 dahingehend präzisiert, dass sie in ihrer Funktion als Auftragsverarbeiterin die Datenschutzpflichten nach Art. 28 Abs. 3 lit. a bis h DSGVO treffen.

Zu Art. 80 Z 9 (§ 55 Abs. 1 bis 3 WaffG):

Zu Abs. 1:

Im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie das in der DSGVO normierte Transparenzgebot (vgl. ErwGr 60 zur DSGVO; siehe auch Art. 5 DSGVO), soll im Einleitungsteil des Abs. 1 der Zweck der Datenverarbeitung festgelegt werden.

Art. 26 DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 55 entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der Zentralen Informationssammlung verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden. Zudem soll im letzten Satz eine terminologische Anpassung erfolgen, da in der DSGVO (Art. 4 Z 10) „Dritten“ eine andere Bedeutung zugrunde gelegt wird. Dadurch soll sich jedoch keine inhaltliche Änderung im Vergleich zur geltenden Rechtslage ergeben.

Zu Abs. 1a:

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 1a die Zuständigkeit zwischen den gemeinsam Verantwortlichen der Zentralen Informationssammlung dahingehend aufteilen, dass Informations-, Auskunfts-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den

Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier (Abs. 1a) – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Zu Abs. 2:

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf die Zentrale Informationssammlung bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. In dieser Funktion sollen ihn auch die Datenschutzpflichten nach Art. 28 Abs. 3 lit a bis h DSGVO treffen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 3:

Der gemäß § 32 ermächtigte Gewerbetreibende trifft im Zuge der Registrierung die gesetzlich determinierte Entscheidung, Daten der betroffenen Person (zB Käufer einer Waffe) zu verarbeiten. Zudem dürfen ihm Daten der betroffenen Person (ua. zu Waffenverboten) übermittelt werden, die wiederum als Entscheidungsgrundlage für sein Handeln (zB Ablehnung eines Geschäfts, Nicht-Aushändigung einer Waffe) dienen sollen. Daher soll Abs. 3 dahingehend präzisiert werden, dass Gewerbetreibende als Verantwortliche nach Art. 4 Z 7 DSGVO tätig werden.

Zu Art. 80 Z 10 (§ 55 Abs. 4 WaffG):

Der erste Satz kann zur Gänze entfallen, da sich die Berechtigung der Waffenbehörden, die in der Zentralen Informationssammlung verarbeiteten Daten zu benützen, bereits aus Abs. 1 ergibt.

Zu Art. 80 Z 16 und 18 (§ 55 Abs. 6 und 9 WaffG):

Da sich das Auskunftsrecht des Betroffenen künftig direkt aus Art. 15 DSGVO ergibt, hat eine Verweisanpassung in Abs. 6 zu erfolgen.

Aufgrund der vorgeschlagenen Protokollierungsregelung in Abs. 10 soll in Abs. 9 eine Verweisanpassung erfolgen.

Zu Art. 80 Z 19 (§ 55 Abs. 10 WaffG):

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, im Rahmen des ZWR in Abs. 10 eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Zu Art. 81 (Änderung des Zivildienstgesetzes 1986)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 1 Z 15 B-VG („Angelegenheiten des Zivildienstes“).

Zu Art. 81 Z 1, 2, 4, 5 und 18 (§ 5 Abs. 2, 3 und 4, § 6 Abs. 4, § 57a Abs. 5 ZDG):

Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im Zivildienstgesetz 1986 verwendeten Begriffe erforderlich erscheint, werden diese nun an die Definitionen der DSGVO (Art. 4 DSGVO) angeglichen. Beispielsweise sollen die Begriffe „einbringen“; „weiterleiten“, „zurücksenden“ und „zur Kenntnis bringen“ von Daten durch „übermitteln“, der Begriff „Einbringung“ durch „Übermittlung“ ersetzt werden.

Zu Art. 81 Z 3 (§ 5 Abs. 3 ZDG):

Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 DSG 2000. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot (vgl. Art. 9 DSGVO), weshalb beabsichtigt ist, von der Verarbeitung des Religionsbekenntnisses künftig abzusehen. Da § 17 Abs. 7 Z 1 und 2 WG 2001, auf den im letzten Satz verwiesen wird, in dieser Form nicht mehr in Geltung steht, soll der letzte Satz entfallen.

Zu Art. 81 Z 6 (§ 6 Abs. 5 ZDG):

Es handelt sich um die Beseitigung eines redaktionellen Versehens.

Zu Art. 81 Z 7, 8, 10 und 11 (§ 8 Abs. 7, § 21 Abs. 5, § 34b Abs. 1 und 3 ZDG):

Da § 7 Abs. 3 nicht mehr in Kraft ist, sollen § 8 Abs. 7, § 21 Abs. 5, § 34b Abs. 1 Z 2 und Abs. 3 entfallen.

Zu Art. 81 Z 9 (§ 31 Abs. 3 ZDG):

Aufgrund der Tatsache, dass dem Unabhängigen Beirat für Zivildienstbeschwerdeangelegenheiten – im Gegensatz zum Zivildienstbeschwerderat – nicht mehr die Beratung des Bundesministers für Inneres vor Erlassung von Verordnungen nach § 31 Abs. 3 obliegt (vgl. § 43), soll die Bestimmung angepasst werden und somit die Anhörung entfallen.

Zu Art. 81 Z 12 und 13 (Überschrift zu Abschnitt IXa, § 57a Abs. 1 ZDG):

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten, weshalb terminologische Anpassungen an die neuen Begrifflichkeiten erfolgen sollen.

Die vorgeschlagenen Ergänzungen dienen – ohne eine inhaltliche Änderung der bisherigen Praxis herbeizuführen – im Wesentlichen dazu, vor allem im Hinblick auf Art. 6 DSGVO betreffend die Rechtmäßigkeit der Verarbeitung sowie auf den im DSGVO vorgesehenen Grundsatz der Transparenz für den Betroffenen (vgl. ErwGr 39 zur DSGVO) eine Konkretisierung der für die Verarbeitung in Betracht kommenden Datenarten herbeizuführen.

Demnach soll die Zivildienstserviceagentur explizit ermächtigt sein, Identitäts- und Erreichbarkeitsdaten (zB Namen, Geburtsdatum, Geburtsort, Familienstand, Vorname der Eltern, Sozialversicherungsnummer, Sterbedatum, Wohnadressen), Daten über die gesundheitliche Eignung (zB Körpergröße, Gewicht, Blutgruppe, Brillenträger, Gutachten von Amtsärzten gemäß §§ 9 und 19, sonstige Gesundheitsdaten), Daten über besondere Kenntnisse und Fähigkeiten (zB Beruf, Schulbildung), das bereichsspezifische Personenkennzeichen (vgl. § 9 E-Government-Gesetz), Daten, die für die Ableistung des ordentlichen Zivildienstes erforderlich sind (zB Fahrtkosten, Bescheid über Zuerkennung von Wohnkostenbeihilfe, Bescheid über Zuerkennung von Familienunterhalt, Wohnkostenbeihilfe, Familienunterhalt), Daten für die Abwicklung von Personalangelegenheiten vor oder während der Ableistung des ordentlichen Zivildienstes, wie Versetzung, Nichteinrechnung, Unterbrechung, Anzeigen wegen Nichtantritt des Zivildienstes, Entlassung, Verfahren betreffend die Aufhebung der Zivildienstpflicht sowie Abwesenheiten (zB aufgrund von Unfall oder Krankheit), Daten zum Erlöschen der Zivildienstpflicht (zB Bescheide, Nachweise, Daten der Sozialversicherungsträger), Bezeichnung, Adresse und sonstige Daten zu Rechtsträgern und Einrichtungen, Daten des Verfahrens zur Feststellung und zum Widerruf der Zivildienstpflicht (zB Antragsdatum, Bezeichnung der Militärbehörde, Datum und Ergebnis der Strafregisterauskunft), Daten des Verfahrens zur Zuweisung zur Ableistung des ordentlichen Zivildienstes (zB Dienstantrittsdatum, zu erbringende Dienstleistungen) sowie Daten für die Abwicklung eines Aufschubs- und Befreiungsverfahrens (zB Begründung für Befreiung bzw. Aufschub, Dauer der Befreiung bzw. Aufschub) zu verarbeiten.

Zu Art. 81 Z 14 und 15 (§ 57a Abs. 1a und Abs. 2 ZDG):

Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 DSG 2000. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Im gegebenen Zusammenhang ist der Tatbestand des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Datenverarbeitung der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten öffentlichen Interesses dienen muss. Im Hinblick darauf, dass Daten über die gesundheitliche Eignung den besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) zuzuordnen sind und die Erforderlichkeit besteht, bei deren Verarbeitung spezifische Maßnahmen zur Wahrung der Grundrechte

und Interessen der betroffenen Person vorzusehen (vgl. Art. 9 Abs. 2 lit. g DSGVO), soll explizit normiert werden, dass eine Verarbeitung von Daten über die gesundheitliche Eignung nur für Zwecke der Feststellung der gesundheitlichen Eignung zur Dienstleistung (zB tauglich, untauglich) und insoweit zulässig ist, als dies für die Zivildienstverwaltung unerlässlich ist. Diese Daten sollen außerdem lediglich manuell und nicht automationsunterstützt verarbeitet werden dürfen.

Zudem soll in Abs. 2 ausdrücklich geregelt werden, dass eine Übermittlung von Daten über die gesundheitliche Eignung an die in Abs. 3 genannten Empfänger jedenfalls unzulässig ist.

Zu Art. 81 Z 17 (§ 57a Abs. 3 Z 3 ZDG):

Da seit 1. Jänner 2014 (Inkrafttreten der Verwaltungsgerichtsbarkeitsnovelle 2012, BGBl. I Nr. 10/2013) das Bundesverwaltungsgericht über Beschwerden gegen Bescheide der Zivildienstserviceagentur entscheidet, sollen in Z 3 die Übermittlungsempfänger um das Bundesverwaltungsgericht erweitert werden. Im Rahmen von Strafverfahren gemäß §§ 58 und 59 oder betreffend Auskünfte in Zusammenhang mit Verfahren gemäß § 6 Abs. 3 ist zudem eine Datenübermittlung an die ordentlichen Gerichte erforderlich, weshalb vorgeschlagen wird, diese ebenfalls als Übermittlungsempfänger auszuweisen.

Da der Begriff „übermitteln“ in Abs. 2 technologieneutral ist, kann der letzte Satz entfallen (vgl. auch ErwGr 15 zur DSGVO).

Zu Art. 81 Z 19 (§ 57a Abs. 6 und 7 ZDG):

Zu Abs. 6:

§ 14 DSG 2000 sieht 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. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. 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 bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden.

Zu Abs. 7:

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 § 57a Abs. 7 für sämtliche nach dem Zivildienstgesetz 1986 verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Zivildienstwesens ist die Verarbeitung personenbezogener Daten von Zivildienstwerbern und Zivildienstpflichtigen in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Zivildienstwerbern und

Zivildienstpflichtigen verbundenen Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des Zivildienstwesens nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen, da die Datenverarbeitung gemäß § 57a Daten zu sämtlichen Zivildienstwerbern und Zivildienstpflichtigen umfasst.

Einerseits ist die Verarbeitung der Daten gemäß § 57a Abs. 1 Z 1 bis 11 erforderlich, um zu beurteilen, ob der Zivildienst bereits vollständig abgeleistet wurde. Andererseits sind die Daten insbesondere für Zwecke der Zuweisung des Zivildienstpflichtigen zu einem Rechtsträger bzw. zu einer Einrichtung sowie für die Abwicklung der Personalangelegenheiten während der Ableistung des ordentlichen Zivildienstes unbedingt erforderlich. Der generelle Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO ist daher unerlässlich.

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 daher auch bei Ausschluss des Widerspruchsrechts unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 dem Verantwortlichen 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 (zB auf der 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 ordnungsgemäßen Vollzug des Zivildienstgesetzes 1986 gewährleisten.

Zu Art. 81 Z 20 (§ 76b Abs. 12 ZDG):

Da das Religionsbekenntnis den besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) zuzurechnen ist und eine Verarbeitung gemäß Art. 9 Abs. 1 DSGVO grundsätzlich untersagt ist, soll die Verarbeitung des Religionsbekenntnisses durch die Zivildienstserviceagentur nicht mehr zulässig sein (siehe Erläuterungen zu § 5 Abs. 3). Die Daten zum Religionsbekenntnis, die vor Inkrafttreten dieses Bundesgesetzes automationsunterstützt verarbeitet wurden, sind mit Inkrafttreten dieses Bundesgesetzes umgehend zu löschen.

Zu Art. 82 (Änderung des BFA-Verfahrensgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 3 B-VG („Ein- und Auswanderungswesen einschließlich des Aufenthaltsrechtes aus berücksichtigungswürdigen Gründen“; „Aufenthaltsverbot, Ausweisung und Abschiebung“; „Asyl“).

Zu Art. 82 Z 1, 2 und 3 (Inhaltsverzeichnis):

Die Änderungen stellen eine notwendige Adaptierung des Inhaltsverzeichnisses dar.

Zu Art. 82 Z 4 (§ 2 Abs. 2 BFA-VG):

Zur besseren Verständlichkeit wird für den Anwendungsbereich des BFA-VG auf die Definition der DSGVO gemäß dem vorgeschlagenen § 2 Abs. 4 Z 24 FPG verwiesen.

Zu Art. 82 Z 5 (§ 13 Abs. 1 BFA-VG):

Da sich die Verpflichtung des Fremden zur Mitwirkung an einer erkennungsdienstlichen Behandlung bereits aus dem in § 24 Abs. 4 verwiesenen § 65 Abs. 4 SPG ergibt, kann deren Normierung in § 13 Abs. 1 entfallen.

Zu Art. 82 Z 6 bis 8 und 18 (Überschriften der §§ 23, 27 und 32 BFA-VG; §§ 23 Abs. 1 und 2, 27 Abs. 3 BFA-VG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO.

Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich der DSGVO der „Verantwortliche“ bzw. „gemeinsam Verantwortliche“ (Art. 4 Z 7 und 26 Abs. 1 DSGVO) einer Datenverarbeitung.

Zu Art. 82 Z 9 und 10 (§ 23 Abs. 3 bis 6 BFA-VG):

Zu Abs. 3:

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung wird im vorgeschlagenen § 23 Abs. 3 Gebrauch gemacht. Für einen geordneten Vollzug des Asyl- und Fremdenwesens ist die Verarbeitung personenbezogener Daten von Fremden in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, einen generellen Ausschluss des Widerspruchsrechts nach Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen.

Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den betroffenen Fremden eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der betroffene Fremde die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Fremden verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden und dem Verwaltungsgericht übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehener Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der –

wenn auch nur vorübergehenden – Unzulässigkeit einer Weiterverarbeitung nicht mehr gewährleistet, dass die Behörde oder das Verwaltungsgericht sämtliche Daten und Informationen, die es für eine rechtsrichtige Entscheidung benötigt, tatsächlich heranziehen kann. Dies könnte in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren bzw. würde eine Verfahrensführung (Ermittlungsverfahren zu diversen Tatbestandsmerkmalen in asyl- und fremdenrechtlichen Normen) geradezu unmöglich machen. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechtes sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

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 personenbezogenen Daten, 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 und 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher kein Rechtsschutzdefizit und stellt die Bestimmung eine ausgewogene Abwägung zwischen den administrativen Interessen und dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar.

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 über den Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung zu informieren sind. Ausdrücklich steht es den Verantwortlichen 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 der Homepage des Bundesamtes bzw. des BVwG).

Zu Abs. 4 und 5:

Der vorgeschlagene Abs. 4 schränkt das Auskunftsrecht des Betroffenen (Art. 15 DSGVO) in Übereinstimmung mit Art. 23 DSGVO nur in jenen Fällen ein, in denen der Auskunft eines der in Z 1 bis 5 genannten, wichtigen Ziele des allgemeinen öffentlichen Interesses entgegensteht.

Entsprechend Art. 23 Abs. 2 lit. h DSGVO sieht der vorgeschlagene Abs. 5 als Grundsatz vor, dass der Betroffene über die Einschränkung oder Verweigerung der Auskunft sowie über den dafür maßgeblichen Grund zu informieren ist, die Erteilung dieser Information jedoch in bestimmten Ausnahmefällen unterbleiben kann. Dabei wird von der Behörde im Einzelfall abzuwägen sein, ob die Erteilung der Information den konkreten Zweck bzw. die konkrete Maßnahme, zu dem (der) bestimmte Daten verarbeitet wurden, etwa eine – den Betroffenen einbeziehende – Maßnahme der Erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1 des Polizeilichen Staatsschutzgesetzes – PStSG, BGBl. I Nr. 5/2016), gefährden könnte. Zum Schutz der Interessen des Betroffenen ist als grundrechtsschützende Maßnahme vorgesehen, dass die für die Nichterteilung der Auskunft maßgeblichen Gründe mit Aktenvermerk festzuhalten sind.

Zu Abs. 6:

Abs. 6 entspricht inhaltlich dem Abs. 3 der geltenden Rechtslage. Es wurde lediglich ein redaktionelles Versehen beseitigt.

Zu Art. 82 Z 11 (§ 24 Abs. 1 Einleitungsteil und Z 2):

In Umsetzung der DSGVO wird im Einleitungsteil des § 24 Abs. 1 der konkrete Zweck einer erkennungsdienstlichen Behandlung festgelegt.

§ 24 Abs. 1 Z 2 in seiner geltenden Fassung wurde mit dem Fremdenbehördenneustrukturierungsgesetz, BGBl. I Nr. 87/2012, eingeführt. Der darin enthaltene Verweis bezog sich zum Zeitpunkt des Inkrafttretens des Fremdenbehördenneustrukturierungsgesetzes auf § 3 Abs. 4 AsylG 2005 in der Fassung BGBl. I Nr. 87/2012, welcher die amtswegige Zuerkennung des internationalen Schutzes aufgrund völkerrechtlicher Verpflichtungen Österreichs regelte. Mit Inkrafttreten des Fremdenrechtsänderungsgesetzes 2015, BGBl. I Nr. 70/2015, wurde die oz. Bestimmung des § 3 Abs. 4 AsylG 2005 inhaltsgleich in § 3a AsylG 2005 übernommen, der Verweis in § 24 Abs. 1 Z 2 jedoch nicht entsprechend angepasst. Mit der vorgeschlagenen Änderung soll dieses redaktionelle Versehen nunmehr beseitigt werden.

Zu Art. 82 Z 12 (§ 24 Abs. 3a BFA-VG):

Die vorgeschlagene Änderung dient der Anpassung der für die erkennungsdienstliche Behandlung geltenden Voraussetzungen an die Vorgaben der DSGVO. Da eine erkennungsdienstliche Behandlung auch die Abnahme von Papillarlinienabdrücken der Finger und damit die Verarbeitung einer besonderen Kategorie personenbezogener Daten – siehe dazu auch die Erläuterungen zu § 28 Abs. 4 – umfassen kann, sind gemäß Art. 9 Abs. 2 lit. g DSGVO spezifische grundrechtsschützende Maßnahmen zu Gunsten des Betroffenen vorzusehen. Es wird daher vorgeschlagen, die Vornahme der erkennungsdienstlichen Behandlung, soweit sie insbesondere auch die Abnahme von Papillarlinienabdrücken der Finger umfasst, ausschließlich geeigneten und besonders geschulten Bediensteten des Bundesamtes, der Landespolizeidirektionen und der Vertretungsbehörden vorzubehalten, welche der Verschwiegenheitspflicht unterliegen. Handelt es sich bei diesen Bediensteten um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Durchführung einer erkennungsdienstlichen Behandlung durch Bedienstete, für die weder die Vorschriften des BDG noch des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Durchführung erkennungsdienstlicher Behandlungen etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung zur Verschwiegenheit verpflichtet sind. Weiters wird die Durchführung einer erkennungsdienstlichen Behandlung – nach dem bewährten Vorbild des § 13 FPG – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Zu Art. 82 13 (§ 24 Abs. 4 BFA-VG):

Betreffend die erkennungsdienstliche Behandlung von Fremden hat in Umsetzung der DSGVO eine Anpassung der Verweise auf das SPG zu erfolgen.

Zu Art. 82 Z 14 (Überschriften der §§ 26 und 28 BFA-VG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO.

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Dieser hat daher in den Überschriften der §§ 26 und 28 zu entfallen.

Zu Art. 82 Z 15 (§ 26 BFA-VG):

Zu Abs. 1:

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen, durch den Begriff des gemeinsam Verantwortlichen in Art. 26 Abs. 1 DSGVO. § 26 Abs. 1 ist daher entsprechend anzupassen. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der im Zentralen Fremdenregister verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Das Bundesverwaltungsgericht, welches nach bisheriger Rechtslage in Bezug auf das Zentrale Fremdenregister – neben den anderen in Abs. 1 genannten Behörden – als datenschutzrechtlicher Auftraggeber fungierte, wird eine solche Funktion künftig nicht mehr ausüben. In der Neufassung des Abs. 1 wird das Bundesverwaltungsgericht daher nicht in die angeführte Auflistung der iSd Art. 4 Z 7 in Verbindung mit Art. 26 Abs. 1 DSGVO gemeinsam Verantwortlichen aufgenommen. Um jedoch sicherzustellen, dass es auch künftig Zugang zu den im Zentralen Fremdenregister verarbeiteten personenbezogenen Daten erhält, wird vorgesehen, dass ihm diese Daten gemäß § 29 Abs. 1 Z 20 übermittelt werden dürfen, sofern dies zur Erfüllung der ihm übertragenen Aufgaben erforderlich ist.

Zu Abs. 2:

Gemäß Art. 26 Abs. 1 Satz 2 DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – z. B. Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne teilt der vorgeschlagene Abs. 2 die Zuständigkeit zwischen den gemeinsam Verantwortlichen des Zentralen Fremdenregisters dahingehend auf, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren (z. B. Asylverfahren nach dem AsylG 2005, Verfahren zur Erteilung eines Aufenthaltstitels nach dem NAG etc.) oder den von ihm gesetzten (verfahrensfreien) Maßnahmen (z. B. Abschiebung oder Entziehung gegenstandslos gewordener Aufenthaltstitelkarten) verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB. das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird. Nimmt ein Betroffener unter Nachweis seiner Identität ein Recht nach der DSGVO gegenüber einem unzuständigen Verantwortlichen wahr, ist er gemäß dem letzten Satz des neuen Abs. 2 an den zuständigen Verantwortlichen zu verweisen.

Zu Abs. 3:

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Fremdenregister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 4:

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO. Die bisher im ersten Satz vorgesehene Sperre des Zugriffs auf im Zentralen Fremdenregister verarbeitete personenbezogene Daten entspricht der Sache nach der „Einschränkung der Verarbeitung“ dieser Daten gemäß Art. 4 Z 3 DSGVO. Der vorgeschlagene erste Satz sieht daher bei Wegfall der Speichervoraussetzungen oder der sonstigen Notwendigkeit der (weiteren) Datenverarbeitung die Einschränkung der Verarbeitung der betreffenden Daten vor und normiert die bisher im dritten Satz enthaltene Ausnahme von der Zugriffssperre als jenen Ausnahmefall, auf den die Datenverarbeitung einzuschränken ist. Der zweite Satz kann – abgesehen von der terminologischen Anpassung an Art. 4 Z 3 DSGVO – unverändert beibehalten werden.

Zu Abs. 5:

Die vorgeschlagene Änderung dient der terminologischen Anpassung an Art. 4 Z 3 DSGVO. Im Gegensatz zur bisherigen Fassung des ersten Satzes wird nicht mehr ausdrücklich vorausgesetzt, dass sich die nach Ablauf von sechs Jahren eintretende Prüfplicht (lediglich) auf Daten bezieht, deren Verarbeitung noch nicht eingeschränkt ist, weil sich dies bereits aus dem Inhalt und dem Zweck der Prüfung eindeutig ergibt. Die Änderung des zweiten und die Anfügung eines dritten Satzes dienen lediglich der besseren Lesbarkeit, ohne die Rechtslage materiell zu ändern. Der bisherige zweite Satz enthält eine alternative Aufzählung von zwei einander ausschließenden Bedingungen, unter denen ausnahmsweise nicht mit Zugriffssperre und – infolge des Verweises auf Abs. 2 (nunmehr Abs. 4) – nach Ablauf von zwei weiteren Jahren mit physischer Löschung vorzugehen ist. Demgegenüber nennt der vorgeschlagene zweite Satz nur noch den ersten Fall, dass der Speichergrund nach Ablauf der Sechs-Jahres-Frist weiterhin besteht und eine Einschränkung der Verarbeitung daher (noch) nicht in Betracht kommt. Der zweite Fall, dass bereits eine Löschungspflicht gemäß § 23 Abs. 3 besteht und die betreffenden Daten daher sofort und nicht erst im Anschluss an eine zweijährige Einschränkung ihrer Verarbeitung zu löschen sind, ist im vorgeschlagenen dritten Satz genannt.

Zu Abs. 6 und 7:

In Abs. 6 und 7, welche den Abs. 4 und 5 der geltenden Rechtslage entsprechen, wurden keine inhaltlichen Änderungen vorgenommen. Durch die Änderung in Abs. 7 soll lediglich die Schreibweise des Begriffes des „Zentralen Fremdenregisters“ vereinheitlicht und der Verweis auf die Löschungsfristen des neuen § 23 Abs. 6 angepasst werden.

Zu Art. 82 Z 16 (§ 27 Abs. 1 Einleitungs- und Schlussteil):

Die vorgeschlagene Änderung dient – ohne eine materielle Änderung der Rechtslage herbeizuführen – lediglich einer sprachlichen Vereinfachung. Da die Befugnis der gemeinsam Verantwortlichen, personenbezogene Daten Fremder im Zentralen Fremdenregister zu verarbeiten, bereits ausdrücklich in § 26 Abs. 1 normiert ist, kann sich § 27 Abs. 1 auf die Konkretisierung der für eine Verarbeitung in Betracht kommenden Datenarten beschränken.

Zu Art. 82 Z 17 (§ 27 Abs. 1 Z 5, 10, 20 und 21 BFA-VG):

Zu Abs. 1 Z 5:

Auf Grund der vorgeschlagenen Änderung können nicht nur die im Bundesgebiet, sondern auch die außerhalb desselben gelegenen Wohnanschriften des Fremden im Fremdenregister verarbeitet werden. Die Kenntnis – und damit die Verarbeitung – von im Ausland gelegenen Wohnanschriften des Fremden kann sowohl für das Bundesamt als auch für die Vertretungsbehörden und die Behörden nach dem NAG zur Erfüllung ihrer Aufgaben erforderlich sein. So ergehen etwa Entscheidungen der Vertretungsbehörden in Visaangelegenheiten (§ 11 FPG), der Behörden nach dem NAG über die Erteilung von Aufenthaltstiteln in Fällen, in denen kein Recht zur Inlandsantragstellung besteht (§ 21 Abs. 1 NAG), oder des Bundesamtes über die Verkürzung bzw. die Aufhebung eines Einreise- oder Aufenthaltsverbotes (§§ 60 Abs. 1 und 2, 69 Abs. 2 FPG) notwendigerweise gegenüber Fremden, deren Wohnanschrift sich außerhalb des Bundesgebietes befindet.

Zu Abs. 1 Z 10:

Die vorgeschlagene Änderung der Z 10 dient der terminologischen Anpassung an die DSGVO.

Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 DSG 2000. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Im gegebenen Zusammenhang ist der Tatbestand des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Datenverarbeitung der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen muss. Zweck der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Z 10 ist es, den Schutz der Gesundheit oder der körperlichen Unversehrtheit des gegenüber dem betroffenen Fremden einschreitenden Organs oder dritter Personen, die von einer Amtshandlung betroffen sein können, sicherzustellen. Z 10 dient daher der Verwirklichung eines erheblichen öffentlichen Interesses im Sinne des Art. 9 Abs. 2 lit. g DSGVO, das im Übrigen auch in der DSGVO selbst ausdrücklich anerkannt ist (vgl. ErwGr 52 zur DSGVO und insbesondere die darin als Beispiel genannte „Sicherstellung und Überwachung der Gesundheit“).

In den Fällen des – hier einschlägigen – Art. 9 Abs. 2 lit. g DSGVO sind „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ gesetzlich vorzusehen. Diesem Erfordernis wird durch die in Z 10 normierte Voraussetzung, dass die Verarbeitung besonderer Kategorien personenbezogener Daten „zur Wahrung lebenswichtiger Interessen anderer“ notwendig sein muss, und durch die Einschränkung, dass nur Gesundheitsdaten, nicht aber sonstige besondere Kategorien personenbezogener Daten verarbeitet werden dürfen, Rechnung getragen. Die Verarbeitung gemäß Z 10 ist somit von vornherein auf jene personenbezogenen Daten eingeschränkt, deren Kenntnis tatsächlich geeignet ist, den Schutz der Gesundheit oder der körperlichen Unversehrtheit des einschreitenden Organs zu gewährleisten. Die Voraussetzung, dass „lebenswichtige“ Interessen anderer zu wahren sind, schränkt die für eine Bearbeitung in Betracht kommenden Gesundheitsdaten zusätzlich auf ein Minimum ein, sodass ein angemessener Ausgleich zwischen dem Interesse des Betroffenen am Schutz seiner personenbezogenen Daten und dem Interesse des einschreitenden Organs bzw. des von der Amtshandlung in sonstiger Weise betroffenen Dritten gewährleistet ist.

Zur Ersetzung des Begriffs „Verwendung“ durch den Begriff „Verarbeitung“ wird auf die Erläuterungen zu § 23 Abs. 1 verwiesen.

Zu Abs. 1 Z 20 und 21:

Hierbei handelt es sich um rein formale Adaptierungen.

Zu Art. 82 Z 19 und 20 (§ 27 Abs. 4 und 5 BFA-VG):

Der zweite und der letzte Satz des Abs. 4 können wegen des vorgeschlagenen Abs. 5 entfallen.

Die DSGVO enthält keine Bestimmung über Protokollierungsvorschriften, innerstaatliche Regelungen sind daher zulässig. Da die Protokollierungsvorschriften des § 14 DSG 2000 entfallen, sind in jedem Materiengesetz gesonderte Protokollierungsvorschriften vorzusehen, um ein gleichbleibendes Datenschutzniveau zu gewährleisten. Dies erfolgt im BFA-VG durch den vorgeschlagenen Abs. 5, welcher für Protokolldaten wie bisher eine angemessene Aufbewahrungsdauer von drei Jahren festlegt.

Zu Art. 82 Z 21 (§ 28 BFA-VG):

Zu Abs. 1:

Die vorgeschlagene Neufassung des Abs. 1 dient der Anpassung an die Systematik der DSGVO.

Hinsichtlich der Zentralen Verfahrensdatei war das Bundesverwaltungsgericht bisher gemeinsam mit dem Bundesamt dazu ermächtigt, die von ihnen ermittelten Verfahrensdaten gemeinsam zu verarbeiten. Auf Grund der Tatsache, dass das Bundesverwaltungsgericht die von ihm ermittelten Informationen zu anhängigen Verfahren ohnehin in einem separaten, ausschließlich von diesem geführten Datensystem verarbeitet, wurde von der eingeräumten Ermächtigung bisher jedoch kein Gebrauch gemacht. Vor diesem Hintergrund wird vorgeschlagen, dass sich die Ermächtigung zur Verarbeitung von Verfahrensdaten in der Zentralen Verfahrensdatei künftig nur noch auf das Bundesamt beschränken soll. Durch Ergänzung der Z 4 des § 29 Abs. 1 um das Bundesverwaltungsgericht und dessen damit einhergehende Aufnahme in den Kreis der Übermittlungsempfänger hinsichtlich der in der Zentralen Verfahrensdatei – und im Zentralen Fremdenregister – verarbeiteten Daten wird sichergestellt, dass dem Bundesverwaltungsgericht – technikneutral – jederzeit derartige Daten übermittelt werden dürfen, sofern diese zur Erfüllung der ihm übertragenen Aufgaben benötigt werden.

Zu Abs. 2:

Der vorgeschlagene Abs. 2 dient der Anpassung an die Systematik und Terminologie der DSGVO. Siehe dazu die Erläuterungen zu § 26 Abs. 3.

Zu Abs. 3:

Die Änderung stellt eine Anpassung an die Neufassung des Abs. 1 dar.

Zu Abs. 4:

Die vorgeschlagene Änderung regelt die Berechtigung zur Datenabfrage aus der Zentralen Verfahrensdatei neu und orientiert sich dabei an der für das Zentrale Fremdenregister geltenden Bestimmung (§ 27 Abs. 2). Die bislang im ersten Satz enthaltene Einschränkung (*„soweit dies ... erforderlich ist“*) führt – bei wörtlicher Auslegung – dazu, dass z. B. für die Erfüllung einer Amtshilfepflicht (Art. 22 B-VG) keine Abfrage aus der Zentralen Verfahrensdatei zulässig wäre. Ebenso lässt sie es als zweifelhaft erscheinen, ob zum Zwecke einer Datenübermittlung an einen Empfänger gemäß § 29 Abs. 1 eine Abfrage zulässig ist, weil die zuletzt genannte Bestimmung keine Pflicht, sondern bloß ein Ermessen des Bundesamtes und insoweit keine gesetzlich übertragene „Aufgabe“ normiert. Es wird daher vorgeschlagen, diese Beschränkung ersatzlos entfallen zu lassen, zumal die Abfrage einen Verarbeitungsvorgang im Sinne des Art. 4 Z 2 DSGVO darstellt und als solcher bereits gemäß § 23 Abs. 1 einer strengen Zweckbindung unterliegt.

Umgekehrt wird – im Hinblick auf die aus Betroffenensicht vergleichbare Sachlage – vorgeschlagen, den letzten Satz des § 27 Abs. 2 zu übernehmen und die Beauskunftung von Papillarlinienabdrücken aus der Zentralen Verfahrensdatei einer entsprechenden Beschränkung zu unterwerfen. Eine derartige Auskunftsbeschränkung ist auch nach der DSGVO geboten, weil Papillarlinienabdrücke der Finger eine besondere Kategorie personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (biometrische Daten) darstellen und daher gemäß Abs. 2 lit. g leg. cit. „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ gesetzlich vorzusehen sind. Die Beschränkung auf Fälle der unbedingten Erforderlichkeit für die Erfüllung einer behördlichen Aufgabe stellt sicher, dass die Beauskunftung von Papillarlinienabdrücken der Finger nur als „ultima ratio“ in Betracht kommt – dh. nur dann stattfindet, wenn eine Erfüllung der behördlichen Aufgabe andernfalls nicht möglich wäre – und überdies einem strengeren Rechtfertigungszwang unterliegt als die Übermittlung sonstiger im Zentralen Fremdenregister verarbeiteter Daten. Dadurch wird dem besonderen Charakter dieser Daten in angemessener Weise Rechnung getragen, ohne die im Einzelfall überwiegenden Verarbeitungsinteressen anderer Behörden zu beeinträchtigen.

Nicht erforderlich ist hingegen eine Übernahme des § 27 Abs. 2 zweiter Satz. Die dort genannten „Daten zur Gültigkeit von Einreise- und Aufenthaltstiteln“, die zum Zweck des Abgleichs mit den Daten des Zentralen Melderegisters (§ 32 Abs. 2) ausnahmsweise als Abfragekriterien herangezogen werden dürfen, werden nämlich ohnehin bereits im Zentralen Fremdenregister gespeichert (§ 27 Abs. 1 Z 11). Es ist

daher nicht erforderlich, auch die in der Zentralen Verfahrensdatei verarbeiteten Daten zum Gegenstand des Abgleichs gemäß § 32 Abs. 2 zu machen.

Zu Abs. 5:

Abs. 5 erster Satz entspricht inhaltlich dem Abs. 4 der geltenden Rechtslage. Es soll lediglich die Schreibweise des Begriffes der „Zentralen Verfahrensdatei“ vereinheitlicht werden und wird der Verweis auf die Löschungsfristen des neuen § 23 Abs. 6 angepasst. Die Einfügung des Wortes „personenbezogene“ hat lediglich klarstelle Funktion. Der neue letzte Satz verdeutlicht die geltende Rechtslage, wonach sich § 28 Abs. 5 auf die Löschung von Daten aus der Zentralen Verfahrensdatei bezieht, für externe Empfänger, denen Daten aus der Zentralen Verfahrensdatei übermittelt werden, gelten die entsprechenden Löschungsvorschriften der jeweiligen Bundes- oder Landesgesetze.

Zu Abs. 6:

Durch den vorgeschlagenen Abs. 6 wird auch für die Zentrale Verfahrensdatei eine Pflicht zur Protokollierung von Abfragen und Datenübermittlungen vorgesehen. Diesbezüglich wird auf die Erläuterungen zu § 27 Abs. 5 verwiesen.

Zu Art. 82 Z 22 (§ 29 Abs. 1 bis 3 BFA-VG):

Die vorgeschlagenen Änderungen haben lediglich klarstellende Funktion.

Zu Art. 82 Z 23 und 24 (§ 29 Abs. 1 Z 4 und 5a BFA-VG):

Zur Aufnahme des Bundesverwaltungsgerichts in den Kreis der Übermittlungsempfänger von gemäß §§ 27 Abs. 1 und 28 verarbeiteten personenbezogenen Daten siehe die Erläuterungen zu den §§ 26 Abs. 1 und 28 Abs. 1.

Durch den Entfall des Verweises auf Art. 148a ff B-VG in § 28 Abs. 3 ist die Volksanwaltschaft als Übermittlungsempfänger in § 29 Abs. 1 zu definieren, um ihr für die Erfüllung ihrer Aufgaben weiterhin den Zugang zu personenbezogenen Daten Fremder zu gewährleisten. Aufgrund der Aufnahme in die Liste der Übermittlungsempfänger gemäß § 29 Abs. 1 dürfen der Volksanwaltschaft – über die bisherige Rechtslage hinausgehend – künftig auch Daten aus dem Zentralen Fremdenregister übermittelt werden, sofern sie diese für die Erfüllung ihrer Aufgaben benötigt. Diese Erweiterung ist vor dem Hintergrund der umfassenden Unterstützungspflicht und des expliziten Ausschlusses der Amtsverschwiegenheit gemäß Art. 148b Abs. 1 B-VG auch verfassungsrechtlich geboten. Eine Schlechterstellung der Volksanwaltschaft gegenüber der bisherigen Rechtslage ist damit nicht verbunden, weil Datenübermittlungen auch in Form der Einräumung und Inanspruchnahme einer Abfrageberechtigung stattfinden können und § 29 nicht regelt, in welcher Form die Daten zu übermitteln sind.

Zu Art. 82 Z 25 (§ 29 Abs. 1 Z 19 BFA-VG):

Im Hinblick auf die Zentrale Verfahrensdatei (§ 28) übt der Bundesminister für Inneres künftig die Funktion des Auftragsverarbeiters gemäß Art. 4 Z 8 in Verbindung mit Art. 28 Abs. 1 DSGVO aus. Ein Zugriff auf sämtliche in der Zentralen Verfahrensdatei verarbeiteten personenbezogenen Daten ist für ihn in dieser Funktion nicht vorgesehen. Ein solcher erscheint jedoch vor dem Hintergrund, dass es sich beim Bundesminister für Inneres um die sachlich in Betracht kommende Oberbehörde handelt, in deren Funktion beispielsweise Stellungnahmen in Verfahren vor dem Europäischen Gerichtshof für Menschenrechte abzugeben sind, zweckmäßig und erforderlich. Aus diesem Grund wurde durch Anfügung der neuen Z 19 eine Rechtsgrundlage für die Übermittlung der nach § 28 verarbeiteten personenbezogenen Daten an den Bundesminister für Inneres geschaffen.

Zu Art. 82 Z 26 und 27 (§ 29 Abs. 2 und 3 BFA-VG):

Soweit die in § 29 Abs. 2 und 3 genannten Empfänger das künftig gemäß § 27 Abs. 1 Z 21 verarbeitete bereichsspezifische Personenkennzeichen (bPK) eines Fremden zur Erfüllung der ihnen übertragenen Aufgaben benötigen, darf dieses gemäß den vorgeschlagenen Änderungen in Abs. 2 und 3 ebenfalls übermittelt werden.

Durch die vorgeschlagene Z 6 in Abs. 2 können Daten des Zentralen Fremdenregisters (§ 27) und der Zentralen Verfahrensdatei (§ 28) in dem gemäß Abs. 2 eingeschränkten Umfang auch den für die Gewährung von Sozial- oder sonstigen Transferleistungen zuständigen Stellen übermittelt werden. Die Notwendigkeit einer solchen Übermittlungsbefugnis ergibt sich daraus, dass bspw. das Mindestsicherungsrecht in den Bundesländern, soweit es Fremde in den Kreis der Anspruchsberechtigten aufnimmt, regelmäßig voraussetzt, dass diesen Fremden ein qualifizierter Aufenthaltsstatus, etwa jener des Asyl- oder des subsidiär Schutzberechtigten, zukommt und sie überdies ihren Wohnsitz oder gewöhnlichen Aufenthalt in dem betreffenden Bundesland genommen haben. Eine Änderung des Aufenthaltsstatus und des Wohnsitzes, wie sie im Fremdenregister und der Verfahrensdatei verarbeitet

wird, kann sich daher – in Verbindung mit sonstigen, zur eindeutigen Identifizierung regelmäßig notwendigen Personaldaten des betreffenden Fremden – unmittelbar auf den Anspruch auf Leistungen der Mindestsicherung auswirken. Gleiches gilt im Zusammenhang mit sonstigen Sozial- oder Transferleistungen, auf deren Gewährung durch Erhalt eines bestimmten asyl- oder fremdenrechtlichen Status ein Anspruch entstehen kann. Aus diesem Grund wird vorgeschlagen, die für die Gewährung von Sozial- oder sonstigen Transferleistungen zuständigen Stellen in den Kreis der Übermittlungsempfänger aufzunehmen.

Zu Art. 82 Z 28 (§ 30 Abs. 6 BFA-VG):

Durch die vorgeschlagene Änderung werden die Staatsbürgerschaftsbehörden verpflichtet, das Bundesamt auch vom Verlust der Staatsbürgerschaft gemäß dem III. Abschnitt des Staatsbürgerschaftsgesetzes 1985 – StbG, BGBl. Nr. 311/1985, in Kenntnis zu setzen, wobei der Verweis auf § 26 StbG klarstellt, dass sich die Informationspflicht auf sämtliche Verlusttatbestände (Erwerb einer fremden Staatsangehörigkeit, Eintritt in den Militärdienst eines fremden Staates, Entziehung und Verzicht) erstreckt. Dies soll dem Bundesamt die durch den Verlust der Staatsbürgerschaft notwendig werdende Prüfung, ob eine aufenthaltsbeendende Maßnahme zu erlassen oder ein Aufenthaltstitel aus berücksichtigungswürdigen Gründen nach dem 7. Hauptstück des AsylG 2005 zu erteilen ist, erleichtern und dient insofern der Sicherstellung eines effizienten Vollzugs des Fremdenwesens. Hinsichtlich des geltenden Abs. 4 zweiter Satz wird angemerkt, dass diesem zufolge die in Abs. 4 Satz 1 genannten Behörden auch gegenüber dem Österreichischen Integrationsfonds ermächtigt und auf Anfrage verpflichtet sind, die in § 27 Abs. 1 Z 1 bis 6 und Z 19 genannten Datenarten zu übermitteln, sofern der Österreichische Integrationsfonds die Daten für die Durchführung von Maßnahmen der Integrationshilfe (§ 68 AsylG 2005) benötigt.

Zu Art. 82 Z 29 (§ 31 Abs. 3 BFA-VG):

Hierbei handelt es sich lediglich um eine Verweisanpassung und eine Anpassung der Terminologie.

Zu Art. 82 Z 30 bis 35 (§ 33 BFA-VG):

Zu Abs. 1:

Die vorgeschlagene Änderung dient der Anpassung an die Vorgaben der DSGVO.

Das bisher in Abs. 1 enthaltene Erfordernis eines mit Österreich vergleichbaren Datenschutzniveaus kann, soweit es sich um die Datenübermittlung an Empfänger in einem Mitgliedstaat handelt, entfallen, weil das Datenschutzniveau innerhalb der Europäischen Union durch die DSGVO harmonisiert ist. Soweit es sich um die Datenübermittlung an Empfänger in einem Drittland handelt, ist zu beachten, dass nach dem V. Kapitel der DSGVO Daten an Empfänger in einem Drittland unter gewissen Voraussetzungen auch dann übermittelt werden können, wenn kein auf das betreffende Drittland lautender Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO vorliegt und es daher unsicher ist, ob dieses Drittland ein dem österreichischen vergleichbares Datenschutzniveau aufweist. Um den von der DSGVO gebotenen Spielraum voll ausschöpfen zu können, hat der Verweis auf das Erfordernis eines vergleichbaren Datenschutzniveaus auch vor diesem Hintergrund zu entfallen.

Der vorgeschlagene Entfall des sprachlich missglückten Verweises auf die „in § 29 genannten Zwecke“ – genauer: auf ausländische, als Übermittlungsempfänger in Betracht kommende Stellen, welche dieselben Zwecke wie die in § 29 genannten, im Inland ansässigen Empfänger verfolgen – dient der Angleichung an die Parallelvorschriften des § 108 Abs. 1 FPG und des § 38 Abs. 1 NAG, die eine vergleichbare Einschränkung nicht vorsehen. Mit Inkrafttreten der DSGVO ist dieser Verweis auch insoweit nicht mehr erforderlich, als eine gemäß § 33 Abs. 1 geschlossene Vereinbarung die Datenübermittlung an Empfänger in einem Drittland ermöglicht. Denn entweder schränkt bereits der gemäß Art. 45 DSGVO grundsätzlich erforderliche Angemessenheitsbeschluss der Europäischen Kommission seinen Geltungsbereich auf „spezifische Sektoren“ (dh. bestimmte Übermittlungsempfänger) im betreffenden Drittland ein, so dass es einer im nationalen Recht normierten Einschränkung des Empfängerkreises nicht mehr bedarf. Oder die Datenübermittlung an das Drittland ist – mangels eines Angemessenheitsbeschlusses und „geeigneter Garantien“ gemäß Art. 46 DSGVO – nur unter den Voraussetzungen des Art. 49 DSGVO zulässig. In einem solchen Fall ist es gemäß Abs. 1 lit. d leg. cit. unter anderem erforderlich, dass die Datenübermittlung an das Drittland einem – im Unions- oder innerstaatlichen Recht anerkannten – öffentlichen Interesse dient. Schließt aber bereits § 29 die Datenübermittlung an bestimmte innerstaatliche Empfänger aus, so bedeutet dies, dass er insoweit ein „öffentliches Interesse“ an der Datenübermittlung gerade nicht anerkennt und die Datenübermittlung an im Drittland befindliche Empfänger mit vergleichbaren Zwecken bzw. vergleichbarer Aufgabenstellung daher auch nicht auf Art. 49 Abs. 1 lit. d DSGVO gestützt werden könnte, ohne dass dies noch explizit im nationalen Recht zu normieren wäre.

Zu Abs. 2:

Die vorgeschlagene Änderung dient der Bereinigung eines redaktionellen Versehens und der terminologischen Anpassung an Art. 4 Z 2 DSGVO.

Zu Abs. 3 und 4:

Die vorgeschlagenen Änderungen sollen klarstellen, dass eine Übermittlung personenbezogener Daten an die für den Fremden zuständige ausländische Behörde (§ 46 Abs. 2 bis 2b FPG) zum Zweck der Beschaffung eines Ersatzreisedokumentes oder einer vergleichbaren, für die Abschiebung bzw. die Einreise in den Herkunfts- oder sonstigen Zielstaat erforderlichen Bewilligung in Verwirklichung eines wichtigen öffentlichen Interesses gemäß Art. 49 Abs. 1 lit. d DSGVO – nämlich der Sicherstellung eines geordneten und effizienten Vollzugs im Asyl- und Fremdenwesen – stattfindet und daher jedenfalls – dh. unabhängig davon, ob in Bezug auf den betreffenden Zielstaat ein Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO) oder sonstige Garantien (Art. 46 DSGVO) vorliegen – zulässig ist.

Zu Abs. 5:

Die vorgeschlagene Änderung trägt dem mit der Verwaltungsgerichtsbarkeits-Novelle 2012, BGBl. I Nr. 51/2012, und dem Verwaltungsgerichtsbarkeits-Ausführungsgesetz 2013, BGBl. I Nr. 33/2013, einhergehenden Entfall des behördlichen Instanzenzuges Rechnung. Die Neufassung des bisher in Z 3 enthaltenen letzten Satzes als Schlussteil der gesamten Bestimmung soll klarstellen, dass der Umstand, dass ein Antrag auf internationalen Schutz gestellt wurde, auch bei Datenübermittlungen gemäß Z 1 oder 2 nicht hervorkommen darf.

Zu Art. 82 Z 36 (§ 56 Abs. 11 BFA-VG):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 83 (Änderung des Fremdenpolizeigesetzes 2005)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 3 B-VG („Regelung und Überwachung des Eintrittes in das Bundesgebiet und des Austrittes aus ihm“; „Aufenthaltsverbot, Ausweisung und Abschiebung“).

Zu Art. 83 Z 1 bis 4 (Inhaltsverzeichnis):

Die Änderungen stellen eine notwendige Adaptierung des Inhaltsverzeichnisses dar.

Zu Art. 83 Z 5 (§ 2 Abs. 4 Z 24 FPG):

Zur besseren Verständlichkeit wird die DSGVO definiert.

Zu Art. 83 Z 6, 7, 8 und 9 (Überschriften zu §§ 98, 99 und 107 FPG; § 98 Abs. 1 bis 6 FPG):

Die vorgeschlagenen Änderungen stellen zunächst terminologische Anpassungen an die DSGVO dar. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Da das Wort „Dritter“ in Art. 4 Z 10 DSGVO mit einer anderen Bedeutung als hier verwendet definiert ist, wird ferner vorgeschlagen, nunmehr von „dritten Personen“ zu sprechen. Eine inhaltliche Änderung ist damit nicht verbunden. Die Aufnahme der Vertretungsbehörden in § 98 Abs. 1 und 2 dient der Bereinigung eines legistischen Versehens.

Durch die vorgeschlagenen Abs. 3 bis 5 wird auch für die nach dem Fremdenpolizeigesetz verarbeiteten Daten das Widerspruchsrecht, das Recht auf Einschränkung der Verarbeitung sowie das Auskunftsrecht der Betroffenen (Art. 21, 18 und 15 DSGVO) eingeschränkt.

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von der Möglichkeit einer solchen Beschränkung wird durch den vorgeschlagenen Abs. 3 Gebrauch gemacht. Für einen geordneten Vollzug des Fremdenwesens ist die Verarbeitung personenbezogener Daten von Fremden in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges,

öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, einen generellen Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für die nach dem Fremdenpolizeigesetz verarbeiteten personenbezogenen Daten vorzusehen.

Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den betroffenen Fremden eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der betroffene Fremde die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Fremden verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden und den Verwaltungsgerichten übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehener Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit einer Weiterverarbeitung nicht mehr gewährleistet, dass die Behörden oder die Verwaltungsgerichte sämtliche Daten und Informationen, die sie für eine rechtsrichtige Entscheidung benötigen, tatsächlich heranziehen können. Dies könnte in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren bzw. würde eine Verfahrensführung (Ermittlungsverfahren zu diversen Tatbestandsmerkmalen in fremdenrechtlichen Normen) geradezu unmöglich machen. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechtes sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

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 personenbezogenen Daten, 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 und 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher kein Rechtsschutzdefizit und stellt die Bestimmung eine ausgewogene Abwägung zwischen den administrativen Interessen und dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar.

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 über den Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung zu informieren sind. Ausdrücklich steht es den Verantwortlichen 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 der Homepage).

Zur Einschränkung des Auskunftsrechtsrechts (Art. 15 DSGVO) gemäß den vorgeschlagenen Abs. 4 und 5 wird auf die Erläuterungen zu § 23 Abs. 4 und 5 BFA-VG verwiesen.

Zum Zweck der verbesserten Übersichtlichkeit wird die Löschungsvorschrift inhaltlich unverändert aus dem bisherigen Abs. 2 herausgelöst und in einem neuen Abs. 6 geregelt.

Zu Art. 83 Z 10 (§ 99 Abs. 1 FPG):

In Umsetzung der DSGVO wird in § 99 Abs. 1 der konkrete Zweck einer erkennungsdienstlichen Behandlung festgelegt.

Zu Art. 83 Z 11 (§ 99 Abs. 2a FPG):

Die vorgeschlagene Änderung dient der Anpassung der für die erkennungsdienstliche Behandlung geltenden Voraussetzungen an die Vorgaben der DSGVO. Da eine erkennungsdienstliche Behandlung auch die Abnahme von Papillarlinienabdrücken der Finger und damit die Verarbeitung einer besonderen Kategorie personenbezogener Daten umfassen kann, sind gemäß Art. 9 Abs. 2 lit. g DSGVO spezifische grundrechtsschützende Maßnahmen zu Gunsten des Betroffenen vorzusehen. Es wird daher vorgeschlagen, die Vornahme der erkennungsdienstlichen Behandlung ausschließlich geeigneten und besonders geschulten Bediensteten der Landespolizeidirektionen und der Vertretungsbehörden vorzubehalten. Handelt es sich bei diesen Bediensteten um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Durchführung einer erkennungsdienstlichen Behandlung durch Bedienstete, für die weder die Vorschriften des BDG noch jene des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Durchführung erkennungsdienstlicher Behandlungen etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung zur Verschwiegenheit verpflichtet sind. Weiters wird die Durchführung einer erkennungsdienstlichen Behandlung – nach dem bewährten Vorbild des § 13 – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Zu Art. 83 Z 12 (§ 99 Abs. 5 FPG):

Betreffend die erkennungsdienstliche Behandlung von Fremden hat in Umsetzung der DSGVO eine Anpassung der Verweise auf das SPG zu erfolgen.

Zu Art. 83 Z 13 und 14 (§ 100 Abs. 1 und 4 FPG):

Die Informationspflichten bei Erhebung von personenbezogenen Daten ergeben sich künftig unmittelbar aus Art. 13 f. DSGVO, die bisherigen Bestimmungen zur Information über die Ermittlung erkennungsdienstlicher Daten in Abs. 1 und 4 haben daher zu entfallen. Die Informationspflicht kann so wie bisher durch das Aushändigen von Informationsblättern erfüllt werden, nach wie vor ist dabei danach zu trachten, dass dieses in einer dem Fremden verständlichen Sprache abgefasst ist. Das Verwenden von fremdsprachigen Informationsblättern entspricht auch Art. 12 Abs. 1 DSGVO, wonach Informationen gemäß Art. 13f DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln sind. An der gegenwärtigen Praxis soll sich daher durch den Entfall der diesbezüglichen Bestimmung nichts ändern. Darüber hinaus kann die Normierung der Pflicht des Fremden zur Mitwirkung an einer erkennungsdienstlichen Behandlung im letzten Satz entfallen, weil sich diese bereits aus dem in § 99 Abs. 5 verwiesenen § 65 Abs. 4 SPG ergibt.

Die Aufnahme der Vertretungsbehörden in Abs. 1 dient der Bereinigung eines legistischen Versehens.

Zu Art. 83 Z 15 (§ 102 FPG):

§ 102 kann entfallen, da die Übermittlung personenbezogener Daten aus dem Zentralen Fremdenregister an die darin genannten Empfänger bereits von den Z 1, 2, 8, 10, 11, 12 und 13 des § 29 Abs. 1 BFA-VG, der sich als Übermittlungsermächtigung an alle gemeinsam Verantwortlichen des Fremdenregisters und damit auch an die Landespolizeidirektionen richtet, abgedeckt ist.

Zu Art. 83 Z 16 bis 21 (§ 104 FPG samt Überschrift):

Die vorgeschlagene Änderung der Überschrift dient der terminologischen Anpassung an die DSGVO.

Zu Abs. 1

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen, durch den Begriff des gemeinsam Verantwortlichen in Art. 26 Abs. 1. § 104 Abs. 1 ist daher entsprechend anzupassen. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der Zentralen Verfahrensdatei verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht (vgl. die Definition des Informationsverbundsystems in § 4 Z 13 DSG 2000), ist damit nicht verbunden.

Zu Abs. 2:

Gemäß Art. 26 Abs. 1 Satz 2 DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – z. B. Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne teilt der vorgeschlagene (neue) Abs. 2 die Zuständigkeit zwischen den gemeinsam Verantwortlichen der Zentralen Verfahrensdatei dahingehend auf, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren (z. B. Strafverfahren nach dem 2. Abschnitt des 15. Hauptstückes etc.) oder den von ihm gesetzten (verfahrensfreien) Maßnahmen (z. B. Zurückweisungen und Zurückschiebungen) verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB. das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird. Nimmt ein Betroffener unter Nachweis seiner Identität ein Recht nach der DSGVO gegenüber einem unzuständigen Verantwortlichen wahr, ist er gemäß dem letzten Satz des neuen Abs. 2 an den zuständigen Verantwortlichen zu verweisen.

Zu Abs. 3:

Gemäß Art. 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf die Zentrale Verfahrensdatei bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 4:

Abs. 4 entspricht dem Abs. 2 der geltenden Rechtslage.

Zu Abs. 5:

Die vorgeschlagene Änderung regelt die Berechtigung zur Datenabfrage aus der Zentralen Verfahrensdatei neu und orientiert sich dabei an dem für das Zentrale Fremdenregister geltenden § 27 Abs. 2 BFA-VG. Die bislang im ersten Satz enthaltene Einschränkung (*„soweit dies … erforderlich ist“*) führt – bei wörtlicher Auslegung – dazu, dass z. B. für die Erfüllung einer Amtshilfepflicht (Art. 22 B-VG) oder zum Zwecke der Erteilung einer sonstigen Auskunft an einen externen Empfänger, wie sie in manchen Rechtsvorschriften (z. B. in § 158 der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961) vorgesehen ist, keine Abfrage aus der Zentralen Verfahrensdatei zulässig wäre. Es wird daher vorgeschlagen, diese Beschränkung ersatzlos entfallen zu lassen, zumal die Abfrage einen Verarbeitungsvorgang im Sinne des Art. 4 Z 2 DSGVO darstellt und als solcher bereits gemäß § 98 Abs. 1 einer strengen Zweckbindung unterliegt.

Umgekehrt wird – im Hinblick auf die aus der Sicht des Betroffenen vergleichbare Sach- und Interessenlage – vorgeschlagen, den letzten Satz des § 27 Abs. 2 BFA-VG zu übernehmen und die Beauskunftung von Papillarlinienabdrücken aus der Zentralen Verfahrensdatei einer entsprechenden Beschränkung zu unterwerfen. Eine derartige Auskunftsbeschränkung ist auch nach der DSGVO geboten, weil Papillarlinienabdrücke der Finger eine besondere Kategorie personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (biometrische Daten) darstellen und daher gemäß Abs. 2 lit. g leg. cit. „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ gesetzlich vorzusehen sind. Die Beschränkung auf Fälle der unbedingten Erforderlichkeit für die Erfüllung einer behördlichen Aufgabe stellt sicher, dass die Beauskunftung von Papillarlinienabdrücken der Finger nur als „ultima ratio“ in Betracht kommt – d.h. nur dann stattfindet, wenn eine Erfüllung der behördlichen Aufgabe andernfalls nicht möglich wäre – und überdies einem strengeren Rechtfertigungszwang unterliegt als die Übermittlung sonstiger im Zentralen Fremdenregister verarbeiteter Daten. Dadurch wird dem besonderen

Charakter dieser Daten in angemessener Weise Rechnung getragen, ohne die im Einzelfall überwiegenden Verarbeitungsinteressen anderer Behörden zu beeinträchtigen.

Nicht erforderlich ist hingegen eine Übernahme des § 27 Abs. 2 Satz 2 BFA-VG. Die dort genannten „Daten zur Gültigkeit von Einreise- und Aufenthaltstiteln“, die zum Zweck des Abgleichs mit den Daten des Zentralen Melderegisters (§ 32 Abs. 2) ausnahmsweise als Abfragekriterien herangezogen werden dürfen, werden nämlich ohnehin bereits im Zentralen Fremdenregister gespeichert (§ 27 Abs. 1 Z 11). Es ist daher nicht erforderlich, auch die in der Zentralen Verfahrensdatei der Landespolizeidirektionen verarbeiteten Daten zum Gegenstand des Abgleichs gemäß § 32 Abs. 2 BFA-VG zu machen.

Darüber hinaus wird ein redaktionelles Versehen bereinigt.

Zu Abs. 6:

Die vorgeschlagene Änderung des bisherigen Abs. 4 hat lediglich klarstellende Funktion. Der vorgeschlagene letzte Satz trägt dem Verarbeitungsbegriff des Art. 4 Z 2 DSGVO Rechnung. Da der Begriff der „Verarbeitung“ bzw. des „Verarbeitens“ nach dieser Bestimmung – anders als nach § 4 Z 9 DSG 2000 – die Datenübermittlung umfasst, kann sich der im ersten Satz verwiesene § 98 Abs. 6 nunmehr auch auf den Fall beziehen, dass in der Verfahrensdatei verarbeitete personenbezogene Daten zu löschen sind, die nicht nur den Landespolizeidirektionen, sondern auch einem dritten Empfänger, dem sie übermittelt wurden, zur Verfügung stehen. Löschungspflichten und Löschungsfristen richten sich allerdings nur für die Verantwortlichen der Zentralen Verfahrensdatei, also für die Landespolizeidirektionen nach (dem im ersten Satz verwiesenen) § 98 Abs. 6, für einen dritten Empfänger hingegen nach den für diesen geltenden Bestimmungen (etwa nach § 25 Abs. 5 letzter Satz des Arbeitsmarktservicegesetzes – AMSG, BGBl. Nr. 313/1994). Der vorgeschlagene letzte Satz soll klarstellen, dass dies auch dann gilt, wenn ein externer Empfänger die von ihm (weiter-)verarbeiteten Daten ursprünglich aus der Zentralen Verfahrensdatei übermittelt bekommen hat.

Zu Abs. 7:

Die DSGVO enthält keine Bestimmung über Protokollierungsvorschriften, innerstaatliche Regelungen sind daher zulässig. Da die Protokollierungsvorschriften des § 14 DSG 2000 entfallen, sind in jedem Materiengesetz gesonderte Protokollierungsvorschriften vorzusehen um ein gleichbleibendes Datenschutzniveau zu gewährleisten. Dies erfolgt im FPG durch den vorgeschlagenen § 104 Abs. 7.

Zu Art. 83 Z 22 (§ 105 Abs. 1 FPG):

Die vorgeschlagene Änderung dient lediglich der sprachlichen Vereinfachung und bewirkt keine materielle Änderung der Rechtslage.

Zu Art. 83 Z 23 und 24 (§ 108 Abs. 1 und 3 FPG):

Die vorgeschlagenen Änderungen in Abs. 1 dienen lediglich der terminologischen Angleichung an die Parallelvorschrift des § 33 Abs. 1 BFA-VG, ohne eine materielle Änderung der Rechtslage zu bewirken. Bei der Änderung des Abs. 3 handelt es sich um die – zur Vermeidung von Missverständnissen im Hinblick auf § 57 Abs. 3 SPG erforderliche – Bereinigung eines legistischen Versehens.

Zu Art. 83 Z 25 (§ 108 Abs. 4 FPG):

Abs. 4 kann entfallen, da die Datenübermittlung an die für den Fremden zuständige ausländische Behörde (§ 46 Abs. 2 bis 2b) zum Zweck der Beschaffung eines Ersatzreisedokumentes oder einer vergleichbaren, für die Abschiebung bzw. die Einreise in den Herkunfts- oder sonstigen Zielstaat erforderlichen Bewilligung bereits in § 33 Abs. 3 und 4 BFA-VG geregelt ist.

Zu Art. 83 Z 26 (§ 126 Abs. 21 FPG):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 84 (Änderung des Niederlassungs- und Aufenthaltsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 3 B-VG („Ein- und Auswanderungswesen einschließlich des Aufenthaltsrechtes aus berücksichtigungswürdigen Gründen“).

Zu Art. 84 Z 1 bis 3 (Inhaltsverzeichnis):

Die Änderungen stellen eine notwendige Adaptierung des Inhaltsverzeichnisses dar.

Zu Art. 84 Z 4 (§ 2 Abs. 1 Z 21 NAG):

Zur besseren Verständlichkeit wird die DSGVO definiert.

Zu Art. 84 Z 5 bis 8 (Überschrift des 7. Hauptstückes des ersten Teiles, § 34 Abs. 1 bis 6 NAG):

Die vorgeschlagenen Änderungen dienen zunächst der terminologischen Anpassung an die DSGVO. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 DSGVO beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten. Da das Wort „Dritter“ in Art. 4 Z 10 DSGVO mit einer anderen Bedeutung als hier verwendet definiert ist, wird vorgeschlagen, nunmehr von „dritten Personen“ zu sprechen. Eine inhaltliche Änderung ist damit nicht verbunden.

Die Verwaltungsgerichte der Länder sind ebenfalls berechtigt, als gemeinsam Verantwortliche personenbezogene Daten im Rahmen der Zentralen Verfahrensdatei (§ 36) zu verarbeiten und wird daher vorgeschlagen, diese ebenfalls in die allgemeine Bestimmung des § 34 aufzunehmen und sie damit im Rahmen der Verarbeitung personenbezogener Daten nach diesem Bundesgesetz unter anderem auch der Zweckbindung des Abs. 1 zu unterstellen.

Mit Einfügung der neuen Abs. 3 bis 5 wird auch für die nach dem Niederlassungs- und Aufenthaltsgesetz verarbeiteten Daten das Widerspruchsrecht, das Recht auf Einschränkung der Verarbeitung sowie das Auskunftsrecht der Betroffenen (Art. 21, 18 und 15 DSGVO) eingeschränkt.

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von der Möglichkeit einer solchen Beschränkung wird durch den vorgeschlagenen Abs. 3 Gebrauch gemacht. Für einen geordneten Vollzug des Fremdenwesens ist die Verarbeitung personenbezogener Daten von Fremden in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den generellen Ausschluss des Widerspruchsrechts nach Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO auch für die nach dem Niederlassungs- und Aufenthaltsgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den Betroffenen eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten nach diesem Bundesgesetz verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehener Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit einer Weiterverarbeitung nicht mehr gewährleistet, dass die Behörden oder die Verwaltungsgerichte sämtliche Daten und Informationen, die sie für eine rechtsrichtige Entscheidung benötigen, tatsächlich heranziehen können und könnte dies in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren. Für einen geordneten Vollzug des Fremdenwesens und zur Vermeidung von Missbrauch ist es außerdem erforderlich, die gesamte fremdenrechtliche Historie einer Person zu kennen. So kann beispielsweise die Beantragung eines Aufenthaltstitels zum Zweck der Familienzusammenführung im Inland nach Ablehnung der Verlängerung einer Aufenthaltsbewilligung für Studierende ein Hinweis auf möglichen Missbrauch sein. Die Nachvollziehbarkeit der fremdenrechtlichen Historie ist ferner bspw. beim Erwerb eines dauerhaften Aufenthaltsrechts oder bei Ansuchen um Verleihung der österreichischen Staatsbürgerschaft auch im Interesse des Betroffenen gelegen. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

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 personenbezogenen Daten, 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 und 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher kein Rechtsschutzdefizit und stellt die Bestimmung eine ausgewogene Abwägung zwischen den administrativen Interessen und dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar.

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 über den Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung zu informieren sind. Ausdrücklich steht es den Verantwortlichen 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 der Homepage).

Zur Einschränkung des Auskunftsrechtsrechts (Art. 15 DSGVO) gemäß den vorgeschlagenen Abs. 4 und 5 wird auf die Erläuterungen zu § 23 Abs. 4 und 5 BFA-VG verwiesen.

Zum Zweck der verbesserten Übersichtlichkeit wird die Löschungsvorschrift inhaltlich unverändert aus dem bisherigen Abs. 2 herausgelöst und in einem neuen Abs. 6 geregelt.

Zu Art. 84 Z 9 bis 11 (Überschrift zu § 35, § 35 Abs. 1a und 2 NAG):

Die vorgeschlagene Änderung der Überschrift dient der terminologischen Anpassung an die DSGVO.

Die vorgeschlagene Aufnahme des neuen Abs. 1a dient der Anpassung der für die erkennungsdienstliche Behandlung geltenden Voraussetzungen an die Vorgaben der DSGVO. Da eine erkennungsdienstliche Behandlung auch die Abnahme von Papillarlinienabdrücken der Finger und damit die Verarbeitung einer besonderen Kategorie personenbezogener Daten umfassen kann, sind gemäß Art. 9 Abs. 2 lit. g DSGVO spezifische grundrechtsschützende Maßnahmen zu Gunsten des Betroffenen vorzusehen. Es wird daher vorgeschlagen, die Vornahme der erkennungsdienstlichen Behandlung ausschließlich geeigneten und besonders geschulten Bediensteten der Niederlassungs- und Vertretungsbehörden vorzubehalten. Handelt es sich bei diesen Bediensteten um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Durchführung einer erkennungsdienstlichen Behandlung durch Bedienstete, für die weder die Vorschriften des BDG noch des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Durchführung erkennungsdienstlicher Behandlungen etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung zur Verschwiegenheit verpflichtet sind. Weiters wird die Durchführung einer erkennungsdienstlichen Behandlung – nach dem bewährten Vorbild des § 13 FPG – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Betreffend die erkennungsdienstliche Behandlung von Fremden hat in Abs. 2 in Umsetzung der DSGVO eine Anpassung der Verweise auf das SPG zu erfolgen.

Zu Art. 84 Z 12 (§ 36 samt Überschrift NAG):

Die vorgeschlagene Änderung der Überschrift dient der terminologischen Anpassung an die DSGVO.

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Dieser hat daher in der Überschrift des § 36 zu entfallen.

Zu Abs. 1:

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen, durch den Begriff des gemeinsam Verantwortlichen in Art. 26 Abs. 1, was im Wesentlichen dem bisherigen Begriff des „Informationsverbundsystems“ entspricht. § 36 Abs. 1 ist daher entsprechend anzupassen. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der Zentralen Verfahrensdatei verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden. So erfolgt auch die Verarbeitung der Verfahrensdaten durch die Verwaltungsgerichte der Länder weiterhin im Rahmen der Justizverwaltung.

Zu Abs. 2, 3 und 4:

Gemäß Art. 26 Abs. 1 Satz 2 DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – z. B. Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne regelt der vorgeschlagene Abs. 2, dass die Erfüllung von Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstigen Pflichten, welche sich aus der DSGVO ergeben, demjenigen der (gemeinsam) Verantwortlichen obliegt, der diese Daten im Zusammenhang mit von ihm geführten Verfahren verarbeitet hat. Die vorgeschlagene Regelung erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB. das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird. Um zu gewährleisten, dass einem Betroffenen die Wahrnehmung seiner Rechte nicht erschwert wird, verweist ein nach dieser Regelung unzuständiger Verantwortliche den Betroffenen an den zuständigen Verantwortlichen.

Abs. 3 legt fest, dass der Bundesminister für Inneres die Funktion des Auftragsverarbeiters iSd Art. 28 Abs. 1 DSGVO ausübt, was auch der bisherigen Rechtslage (BMI als Betreiber und Dienstleister des bisherigen Informationsverbundsystems) entspricht und nur eine Anpassung an die Terminologie der DSGVO bedeutet. Er übernimmt in dieser Funktion die Verpflichtungen, welche sich aus Art. 28 Abs. 3 lit. a bis h DSGVO ergeben. Diese Bestimmungen sehen beispielsweise geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus vor (Art. 28 Abs. 3 lit. c DSGVO). Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Der vorgeschlagene Abs. 4 entspricht dem Abs. 2 der geltenden Rechtslage.

Zu Abs. 5:

Abs. 3 der geltenden Rechtslage findet sich nunmehr im ersten Satz des vorgeschlagenen Abs. 5. Im Vergleich zum bisherigen Abs. 3 entfällt dabei die Einschränkung, dass eine Abfrage aus der Zentralen Verfahrensdatei nur zur Besorgung einer nach dem NAG übertragenen Aufgabe zulässig ist. Einerseits ist die strenge Zweckbindung der Niederlassungsbehörden und der Landesverwaltungsgerichte bei der Verarbeitung – einschließlich der Abfrage (vgl. Art. 4 Z 2 DSGVO) – von personenbezogenen Daten bereits ausdrücklich in § 34 Abs. 1 normiert, sodass eine Wiederholung dieses Grundsatzes in § 36 unterbleiben kann. Andererseits ist Abs. 3 der geltenden Rechtslage zu eng gefasst, weil er seinem Wortlaut nach – anders als § 34 Abs. 1 – Abfragen zum Zweck der Erfüllung anderer als der im NAG geregelten Aufgaben, insbesondere der Amtshilfepflicht gemäß Art. 22 B-VG und der Unterstützungspflicht gegenüber der Volksanwaltschaft gemäß Art. 148b Abs. 1 B-VG, ausschließt. Darüber hinaus wird ein Redaktionsversehen bereinigt.

Der vorgeschlagene zweite Satz stellt eine weitere, gemäß Art. 9 Abs. 2 lit. g DSGVO notwendige spezifische Maßnahme zur Wahrung der Grundrechte und Interessen von Betroffenen im Zusammenhang

mit der Verarbeitung besonderer Kategorien personenbezogener Daten dar (siehe dazu auch die Erläuterungen zu § 35 Abs. 1a). Nach dem Vorbild des die Datenabfrage aus dem Zentralen Fremdenregister regelnden § 27 Abs. 2 BFA-VG und des vorgeschlagenen § 28 Abs. 4 leg. cit. sollen daher in der Zentralen Verfahrensdatei verarbeitete Papillarlinienabdrücke, welche zu einer besonderen Kategorie personenbezogener Daten gehören, nicht bei jeglicher Abfrage beauskunftet werden, sondern nur dann, wenn die Erfüllung einer behördlichen Aufgabe andernfalls nicht möglich wäre. Dadurch wird dem besonderen Charakter dieser Daten in angemessener Weise Rechnung getragen, ohne die im Einzelfall überwiegenden Verarbeitungsinteressen anderer Behörden zu beeinträchtigen. Im Übrigen wird auf die Erläuterungen zu § 28 Abs. 4 BFA-VG verwiesen.

Zu Abs. 6:

Es wird ein redaktionelles Versehen bereinigt.

Außerdem wird der Verweis auf § 34 Abs. 2 (nunmehr § 34 Abs. 6), der sich auf die dort genannte Löschungspflicht bezieht, präzisiert. Der angefügte Satz verdeutlicht lediglich die geltende Rechtslage, wonach sich § 36 Abs. 6 auf die Löschung von Daten aus der Zentralen Verfahrensdatei bezieht, für externe Empfänger, denen Daten aus der Zentralen Verfahrensdatei übermittelt werden, gelten die entsprechenden Löschungsvorschriften der jeweiligen Bundes- oder Landesgesetze.

Zu Abs. 7:

Der vorgeschlagene Abs. 7 entspricht dem Abs. 5 der geltenden Rechtslage.

Zu Abs. 8:

Die DSGVO enthält keine Bestimmung über Protokollierungsvorschriften, innerstaatliche Regelungen sind daher zulässig. Da die Protokollierungsvorschriften des § 14 DSG 2000 entfallen, sind in jedem Materiengesetz gesonderte Protokollierungsvorschriften vorzusehen um ein gleichbleibendes Datenschutzniveau zu gewährleisten. Dies erfolgt im NAG durch den vorgeschlagenen Abs. 8, welcher für Protokolldaten wie bisher eine angemessene Aufbewahrungsdauer von drei Jahren festlegt.

Zu Art. 84 Z 13 (§ 37 Abs. 1 NAG):

Bei der vorgeschlagenen Änderung handelt es sich lediglich um eine terminologische Anpassung an die DSGVO.

Zu Art. 84 Z 14 (§ 38 Abs. 1 NAG):

Es handelt sich um eine terminologische Anpassung an vergleichbare Bestimmungen in § 33 BFA-VG und § 108 FPG.

Zu Art. 84 Z 15 (§ 38 Abs. 2 NAG):

Es handelt sich um die – zur Vermeidung von Missverständnissen im Hinblick auf § 57 SPG erforderliche – Bereinigung eines redaktionellen Versehens.

Zu Art. 84 Z 16 (§ 38 Abs. 3 NAG):

Da der Begriff der Verarbeitung das Empfangen von Daten einschließt, kann diese Wendung entfallen.

Zu Art. 84 Z 17 und 18 (§ 39 samt Überschrift NAG):

Bei der Änderung der Überschrift handelt es sich um eine terminologische Anpassung an die DSGVO. Die Änderung im Text stellt die Beseitigung eines redaktionellen Versehens dar.

Zu Art. 84 Z 19 (§ 40 Abs. 3 NAG):

§ 40 Abs. 3 hat in der Praxis keine Auswirkungen entfaltet und kann daher ersatzlos entfallen.

Zu Art. 84 Z 20 (§ 82 Abs. 26 NAG):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 85 (Änderung des Grundversorgungsgesetzes-Bund 2005)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 3 B-VG („Asyl“).

Zu Art. 85 Z 1 (§ 1 Z 8 GVG-B 2005):

Zur besseren Verständlichkeit wird die DSGVO definiert.

Zu Art. 85 Z 2 (§ 8 GVG-B 2005 samt Überschrift):

Zu Abs. 1:

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen, durch den Begriff des gemeinsam Verantwortlichen in Art. 26 Abs. 1. Als gemeinsam Verantwortliche iSd DSGVO sind hinsichtlich des Betreuungsinformationssystems nunmehr das Bundesamt als Behörde und die mit der Versorgung von Fremden gemäß Art. 2 Abs. 1 der Grundversorgungsvereinbarung betrauten Dienststellen der Länder – welche nach dem bisherigen Wortlaut des Abs. 1 unter dem Begriff der Behörden zusammengefasst wurden – und der Bundesminister für Inneres vorgesehen. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der im Betreuungsinformationssystem verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Zu Abs. 2 und 3:

Die vorgeschlagenen Abs. 2 und 3 entsprechen den bisherigen Abs. 1a und 2, wobei geringfügige Abweichungen des Wortlauts gegenüber der geltenden Fassung lediglich der sprachlichen Straffung dienen und keine materielle Änderung der Rechtslage bewirken.

Zu Abs. 4 bis 6:

Durch die vorgeschlagenen Abs. 4 bis 6 wird nach dem Vorbild des § 23 Abs. 3 bis 5 BFA-VG auch für die im Betreuungsinformationssystem verarbeiteten Daten das Widerspruchsrecht, das Recht auf Einschränkung der Verarbeitung sowie das Auskunftsrecht des Betroffenen (Art. 21, 18 und 15 DSGVO) eingeschränkt.

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von der Möglichkeit einer solchen Beschränkung wird durch den vorgeschlagenen Abs. 4 Gebrauch gemacht. Für einen geordneten Vollzug des Asyl- und Fremdenwesens und damit auch für die Grundversorgung von Fremden ist die Verarbeitung personenbezogener Daten von Fremden in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, einen generellen Ausschluss des Widerspruchsrechts nach Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen.

Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den Betroffenen eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die lückenlose Verarbeitung von betreuungsrelevanten Daten – beispielsweise über das allfällige Vorliegen eines Sonderbetreuungsbedarfs (medizinische-, psychologische- Besonderheiten, o.ä.) oder über die Gewährung von Leistungen aus der Grundversorgung – ist zur Sicherstellung der öffentlichen Gesundheit und Seuchenprävention sowie zur Wahrung der wirtschaftlichen und finanziellen Interessen Österreichs zu jedem Zeitpunkt erforderlich und damit stets im überwiegenden öffentlichen Interesse gelegen. Eine lückenlose Verarbeitung der Daten dient überdies auch dem Eigeninteresse der Betroffenen. So kann eine Gewährung von Leistungen gemäß Art. 6 der Grundversorgungsvereinbarung, BGBl. I Nr. 80/2004, oder eine Zuweisung von hilfs- und schutzbedürftigen Fremden an die jeweiligen Grundversorgungsstellen der Länder, welche auch die Möglichkeit allfälliger Familienzusammenführungen berücksichtigt, nur dann erfolgen, wenn jederzeit auf die erforderlichen Daten zugegriffen werden kann. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

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 personenbezogenen Daten, 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 und 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher kein Rechtsschutzdefizit und stellt die Bestimmung eine ausgewogene Abwägung zwischen den administrativen Interessen und dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar.

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 über den Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung zu informieren sind. Ausdrücklich steht es den Verantwortlichen 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 der Homepage).

Zur Einschränkung des Auskunftsrechtsrechts (Art. 15 DSGVO) gemäß den vorgeschlagenen Abs. 5 und 6 wird auf die Erläuterungen zu § 23 Abs. 4 und 5 BFA-VG verwiesen.

Zu Abs. 7:

Gemäß § 26 Abs. 1 Satz 2 DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – z. B. Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. Der vorgeschlagene Abs. 7 teilt die Zuständigkeit zwischen den gemeinsam Verantwortlichen dahingehend auf, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB. das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird. Nimmt ein Betroffener unter Nachweis seiner Identität ein Recht nach der DSGVO gegenüber einem unzuständigen Verantwortlichen wahr, ist er gemäß dem letzten Satz des neuen Abs. 7 an den zuständigen Verantwortlichen zu verweisen.

Zu Abs. 8:

Gemäß Art. 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Betreuungsinformationssystem bisher der Bundesminister für Inneres aus, weshalb es im Sinne

größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Abs. 9:

Der vorgeschlagene Abs. 9 entspricht inhaltlich dem Abs. 3 der geltenden Rechtslage mit der Maßgabe, dass der Bundesminister für Inneres die darin genannten Überprüfungen nicht in seiner Funktion als Auftragsverarbeiter vornimmt, sondern – gegenüber dem Bundesamt – in seiner Funktion als zuständiges oberstes Organ (Art. 20 Abs. 1 B-VG) und – gegenüber den Grundversorgungsbehörden der Länder – in seiner Funktion als gemeinsam Verantwortlicher, dem das Überprüfungsrecht durch Abs. 9 eingeräumt wird. Dabei kann der erste Satz des geltenden Abs. 3 entfallen, weil sich die Pflicht der Verantwortlichen, Datensicherheitsmaßnahmen zu ergreifen, künftig unmittelbar aus Art. 32 DSGVO ergibt, auf den zudem im letzten Satz in einem Klammerausdruck verwiesen wird.

Zu Abs. 10:

Der vorgeschlagene Abs. 10 fasst den bisherigen Abs. 3 dahingehend neu, dass von den Ländern entsprechend Art. 4 Abs. 2 der Grundversorgungsvereinbarung beauftragte humanitäre, kirchliche oder private Einrichtungen bzw. Institutionen der freien Wohlfahrtspflege ausdrücklich als Übermittlungsempfänger definiert werden, bezüglich des Hochkommissärs der Vereinten Nationen für Flüchtlinge klargestellt wird, dass ausschließlich dessen Büro in Österreich als Übermittlungsempfänger in Betracht kommt, und das Bundesverwaltungsgericht – im Hinblick auf seine Zuständigkeit als Rechtsmittelinstanz gemäß §§ 7 Abs. 1 Z 1 in Verbindung mit 3 Abs. 2 Z 2 BFA-VG – als neuer Übermittlungsempfänger hinzukommt. Andererseits sollen die Grundversorgungsbehörden der Länder als Übermittlungsempfänger entfallen, weil diese als gemeinsam Verantwortliche des Betreuungsinformationssystems ohnehin Zugriff auf die darin verarbeiteten Daten haben.

Zu Abs. 11:

Abs. 11 entspricht dem Abs. 5 der geltenden Rechtslage mit der Maßgabe, dass sich die Informationspflicht des Hauptverbandes bzw. des jeweils zuständigen Sozialversicherungsträgers nunmehr allgemein auf Fremde, die von einem Land entsprechend der Grundversorgungsvereinbarung betreut werden, erstreckt.

Zu Abs. 12:

In Umsetzung der DSGVO wird in Abs. 12 eine strenge Zweckbindung für Abfragen aus dem Betreuungsinformationssystem festgelegt. Die Formulierung orientiert sich dabei an den für das Zentrale Fremdenregister und die Zentrale Verfahrensdatei geltenden Bestimmungen der §§ 27 Abs. 2 und 28 Abs. 4 BFA-VG. Dabei ist es allerdings nicht erforderlich, Papillarlinienabdrücke als zulässige Abfragekriterien zu definieren, weil diese im Betreuungsinformationssystem nicht verarbeitet werden.

Zu Abs. 13 bis 16:

Abs. 13 bis 16 entsprechen den bisherigen Abs. 6 bis 9.

Zu Abs. 17:

Die DSGVO enthält keine Bestimmung über Protokollierungsvorschriften, innerstaatliche Regelungen sind daher zulässig. Da die Protokollierungsvorschriften des § 14 DSG 2000 entfallen, sind in jedem Materiengesetz gesonderte Protokollierungsvorschriften vorzusehen, um ein gleichbleibendes Datenschutzniveau zu gewährleisten. Dies erfolgt im GVG-B 2005 durch den vorgeschlagenen Abs. 17, welcher für Protokolldaten wie bisher eine angemessene Aufbewahrungsdauer von drei Jahren festlegt.

Zu Art. 85 Z 3 (§ 16 Abs. 22 GVG-B 2005):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 86 (Änderung des Grenzkontrollgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 3 B-VG („Regelung und Überwachung des Eintrittes in das Bundesgebiet und des Austrittes aus ihm“).

Zu Art. 86 Z 1 (Inhaltsverzeichnis):

Die Änderung stellt eine notwendige Adaptierung des Inhaltsverzeichnisses dar.

Zu Art. 86 Z 2 (§ 12 Abs. 2 GrekoG):

Durch den Einsatz der in Abs. 2 Z 2 genannten elektronischen Abfertigungsgeräte (e-Gates) kommt es unter anderem zur Verarbeitung von erkennungsdienstlichen Daten. Erkennungsdienstliche Daten iSd § 2 Abs. 5 Z 4 FPG umfassen mit den Papillarlinienabdrücken der Finger und biometrischen Lichtbildern auch Daten, welche gemäß Art. 9 Abs. 1 der DSGVO als besondere Kategorie personenbezogener Daten gelten. Die in Art. 9 Abs. 1 DSGVO näher bezeichneten besonderen Kategorien personenbezogener Daten entsprechen im Wesentlichen der Kategorie der sensiblen Daten gemäß § 4 Z 2 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999. Die DSGVO normiert für die Verarbeitung solcher Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Im gegebenen Zusammenhang ist der Tatbestand des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Datenverarbeitung der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen muss.

Um zu verdeutlichen, dass Abs. 2 auch zur Verarbeitung solcher besonderen Kategorien personenbezogener Daten ermächtigt, wird ausdrücklich auf die erkennungsdienstlichen Daten hingewiesen.

Die in § 12 Abs. 2 vorgesehenen Mittel werden im Rahmen der Grenzkontrolle und damit im Rahmen der Sicherheitsverwahrung eingesetzt. Diese Unterscheidung ist wichtig, da im Rahmen der Sicherheitsverwaltung die DSGVO, im Rahmen der Sicherheitspolizei jedoch die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI, ABl. L 119 vom 04.05.2016 S. 89 bzw. in deren Umsetzung das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 120/2017 zur Anwendung kommt. Durch die Konkretisierung auf die „Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“, die den Einsatz der Mittel nach Abs. 2 unmittelbar erforderlich machen können, sollen Fehlinterpretationen hinsichtlich der Anwendbarkeit der jeweiligen Bestimmungen vermieden werden.

Zu Art. 86 Z 3 (§ 12a Abs. 2 GrekoG):

Da in § 12a Befugnisse hinsichtlich Identitätsfeststellung und erkennungsdienstliche Behandlung beinhaltet sind, wird auf die Mitwirkungspflicht, die entsprechenden Definitionen zum Erkennungsdienst sowie auf eine Vorschrift zur physischen Löschung von Daten im Sicherheitspolizeigesetz (SPG) verwiesen. Die genannten Bestimmungen finden sich in einem Teil des SPG, welcher sich auf die Verwendung von Daten im Rahmen der Sicherheitspolizei regelt, es wird daher in § 12a Abs. 2 angeordnet, dass an die Stelle der Sicherheitsbehörden (im Rahmen der Sicherheitspolizei), die nach dem Grenzkontrollgesetz zuständigen Behörden (§ 8 Abs. 1 GrekoG) treten.

Zu Art. 86 Z 4 (§ 12a Abs. 3 Z 1 und 2 GrekoG):

Bei den vorgeschlagenen Änderungen handelt sich um die Bereinigung eines legistischen Versehens und um eine terminologische Anpassung an die DSGVO.

Zu Art. 86 Z 5 (§ 12a Abs. 7 GrekoG):

Die vorgeschlagene Änderung dient der Anpassung der für die erkennungsdienstliche Behandlung geltenden Voraussetzungen an die Vorgaben der DSGVO. Da eine erkennungsdienstliche Behandlung auch die Abnahme von Papillarlinienabdrücken der Finger und damit die Verarbeitung einer besonderen Kategorie personenbezogener Daten umfassen kann, sind gemäß Art. 9 Abs. 2 lit. g DSGVO spezifische grundrechtsschützende Maßnahmen zu Gunsten des Betroffenen vorzusehen. Es wird daher vorgeschlagen, die Vornahme der erkennungsdienstlichen Behandlung, soweit sie insbesondere auch die Abnahme von Papillarlinienabdrücken der Finger umfasst, ausschließlich geeigneten und besonders geschulten Bediensteten der Behörde vorzubehalten. Handelt es sich bei diesen Bediensteten um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Durchführung einer erkennungsdienstlichen Behandlung durch Bedienstete, für die weder die Vorschriften des BDG noch des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Durchführung erkennungsdienstlicher Behandlungen etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung zur Verschwiegenheit verpflichtet sind. Weiters wird die Durchführung einer erkennungsdienstlichen Behandlung – nach dem bewährten Vorbild des § 13 FPG – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Zu Art. 86 Z 6 und Z 7 (Überschrift zu § 15 und § 15 Abs. 1 Z 1 GrekoG):

Die vorgeschlagenen Änderungen dienen der Anpassung an die Terminologie der DSGVO.

Zu Art. 86 Z 8 (§ 15 Abs. 1 Z 2 GrekoG):

Hierbei handelt es sich um die Bereinigung eines redaktionellen Versehens.

Zu Art. 86 Z 9 (§ 15 Abs. 2 bis 5 GrekoG):

Durch die vorgeschlagenen Abs. 2 bis 4 wird auch für die nach dem Grenzkontrollgesetz verarbeiteten Daten das Widerspruchsrecht, das Recht auf Einschränkung der Verarbeitung und das Auskunftsrecht der Betroffenen (Art. 21, 18 und 15 DSGVO) eingeschränkt.

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von der Möglichkeit einer solchen Beschränkung wird durch den vorgeschlagenen Abs. 2 Gebrauch gemacht. Für einen geordneten Vollzug des Grenzkontrollwesens (Verordnung (EU) 2016/399 in der Fassung VO (EU) 2017/458 und des Grenzkontrollgesetzes) wie auch des Asyl- und Fremdenwesens ist die Verarbeitung personenbezogener Daten von Reisenden bzw. Fremden in dem gesetzlich vorgesehenen Maße unerlässlich. Eine Grenzkontrolle könnte ohne Abgleich der personenbezogenen Daten mit den entsprechenden Datenbanken nicht ordnungsgemäß vollzogen werden und liegt damit an der Verarbeitung personenbezogener Daten nach diesem Bundesgesetz stets ein überwiegendes öffentliches Interesse vor. Es ist daher erforderlich und sachgerecht, einen generellen Ausschluss des Widerspruchsrechts nach Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen.

Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den Betroffenen eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von Fremden bzw. Reisenden verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehener Löschung – zu jedem Zeitpunkt erforderlich. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechtes sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

Im Übrigen wird ebenso wie zur Einschränkung des Auskunftsrechtsrechts (Art. 15 DSGVO) gemäß den vorgeschlagenen Abs. 3 und 4 auf die Erläuterungen zu § 23 Abs. 3 bis 5 BFA-VG verwiesen.

Der vorgeschlagene Abs. 5 entspricht dem Abs. 2 der geltenden Rechtslage.

Zu Art. 86 Z 10 (§ 18 Abs. 10 GrekoG):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 87 (Änderung des Staatsbürgerschaftsgesetzes 1985)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 11 Abs. 1 Z 1 B-VG („Staatsbürgerschaft“).

Zu Art. 87 Z 1 und 7 (§§ 39a Abs. 1 bis 4 und 56b Abs. 4 StbG):

Die vorgeschlagenen Änderungen in § 39a Abs. 1 und § 56b Abs. 4 dienen zunächst der terminologischen Anpassung an die DSGVO. Der Begriff der Verarbeitung (bzw. des Verarbeitens) personenbezogener Daten umfasst gemäß Art. 4 Z 2 DSGVO sowohl die Verwendung als auch die Speicherung personenbezogener Daten. Werden personenbezogene Daten Dritten zur Verfügung gestellt – nach bisheriger Rechtslage durch die Begriffe „überlassen“ oder „übergeben“ zum Ausdruck gebracht – soll künftig in einheitlicher Weise der Begriff „übermitteln“ verwendet werden.

Durch die vorgeschlagenen Abs. 2 bis 4 wird auch für die nach dem Staatsbürgerschaftsgesetz 1985 verarbeiteten Daten das Widerspruchsrecht, das Recht auf Einschränkung der Verarbeitung sowie das Auskunftsrecht der Betroffenen (Art. 21, 18 und Art. 15 DSGVO) eingeschränkt.

Gemäß Art. 21 Abs. 1 DSGVO haben Betroffene grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus haben Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, den Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung können jedoch gemäß Art. 23 DSGVO zur Sicherstellung eines in Abs. 1 lit. a bis j leg. cit. genannten Zweckes durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung wird im vorgeschlagenen § 39a Abs. 2 Gebrauch gemacht. Im Hinblick auf die zahlreichen Rechte und Pflichten, die an die österreichische Staatsbürgerschaft anknüpfen, insbesondere das Wahlrecht, die Berechtigung zur Teilnahme an Volksbegehren und Volksabstimmungen sowie die Wehrpflicht, liegt es stets im überwiegenden öffentlichen Interesse, dass das Bestehen oder Nichtbestehen der österreichischen Staatsbürgerschaft zu jeder Zeit richtig und zweifelsfrei, also unter Berücksichtigung der vollständigen dafür maßgeblichen Datenlage beauskunftet werden kann. Eine solche Beauskunftung, deren Stellenwert auch durch die umfassenden Mitteilungs- und Informationspflichten gemäß §§ 55, 56 und 56c Abs. 2 zum Ausdruck kommt, setzt die Lückenlosigkeit und Vollständigkeit der nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten voraus. Es ist daher erforderlich und sachgerecht, einen generellen Ausschluss des Widerspruchsrechts nach Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen.

Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch den Betroffenen eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr erfolgen dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Aus den oben angeführten Gründen ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehener Löschung – zu jedem Zeitpunkt erforderlich. Ist die Verarbeitung hingegen unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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. Der generelle Ausschluss des Widerspruchsrechtes sowie des Rechts auf Einschränkung der Verarbeitung, welche auch nach geltender Rechtslage nicht vorgesehen sind, ist daher unerlässlich.

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 personenbezogenen Daten, 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 und 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher kein Rechtsschutzdefizit und stellt die Bestimmung eine ausgewogene Abwägung zwischen den administrativen Interessen und dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar.

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 über den Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung zu informieren sind. Ausdrücklich steht es den Verantwortlichen 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 der Homepage).

Zur Einschränkung des Auskunftsrechtsrechts (Art. 15 DSGVO) gemäß den vorgeschlagenen Abs. 3 und 4 wird auf die Erläuterungen zu § 23 Abs. 4 und 5 BFA-VG verwiesen.

Aufgrund der Einfügung der neuen Abs. 2 bis 4 ändern sich zudem die Absatzbezeichnungen der bisherigen Abs. 2 bis 7 des § 39a.

Zu Art. 87 Z 2 (§ 39a Abs. 5 StbG):

Die vorgeschlagene Änderung dient der Anpassung der für die erkennungsdienstliche Behandlung geltenden Voraussetzungen an die Vorgaben der DSGVO. Da eine erkennungsdienstliche Behandlung auch die Abnahme von Papillarlinienabdrücken der Finger und damit die Verarbeitung einer besonderen Kategorie personenbezogener Daten iSd DSGVO umfassen kann, sind gemäß Art. 9 Abs. 2 lit. g DSGVO spezifische grundrechtsschützende Maßnahmen zu Gunsten des Betroffenen vorzusehen. Es wird daher vorgeschlagen, die Vornahme der erkennungsdienstlichen Behandlung, soweit sie insbesondere auch die Abnahme von Papillarlinienabdrücken der Finger umfasst, ausschließlich geeigneten und besonders geschulten Bediensteten der Staatsbürgerschafts- und Vertretungsbehörden vorzubehalten. Handelt es sich bei diesen Bediensteten um Beamte oder Vertragsbedienstete, ergibt sich die Verschwiegenheitspflicht jeweils unmittelbar aus § 46 des Beamten-Dienstrechtsgesetzes 1979 (BDG), BGBl. Nr. 333/1979, oder §§ 5 oder 79 des Vertragsbedienstetengesetzes 1948 (VBG), BGBl. Nr. 86/1948. Die Durchführung einer erkennungsdienstlichen Behandlung durch Bedienstete, für die weder die Vorschriften des BDG noch des VBG zur Anwendung kommen, darf nur erfolgen, sofern auch diese in Bezug auf die Durchführung erkennungsdienstlicher Behandlungen etwa im Rahmen der Unterzeichnung einer Verschwiegenheitserklärung zur Verschwiegenheit verpflichtet sind. Weiters wird die Durchführung einer erkennungsdienstlichen Behandlung – nach dem bewährten Vorbild des § 13 FPG – durch Verweis auf die Achtung der Menschenwürde und möglichste Schonung der Person ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt.

Zu Art. 87 Z 3 (§ 39a Abs. 6 StbG):

Die Adaptierung der Verweise auf das SPG betreffend die erkennungsdienstliche Behandlung erfolgt auf Grund des neu eingeführten Datenschutzregimes.

Zu Art. 87 Z 4 (§ 56a Abs. 1 StbG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Die Verwendung des Begriffes des „Informationsverbundsystems“ gemäß § 4 Z 13 des Datenschutzgesetzes 2000 (DSG 2000) ist künftig nicht mehr vorgesehen. An dessen Stelle tritt der Begriff der „gemeinsam Verantwortlichen“ (Art. 26 Abs. 1 DSGVO), welche (gemeinsam) die Zwecke und Mittel zur Datenverarbeitung festlegen. In Bezug auf das Zentrale Staatsbürgerschaftsregister (ZSR) sind folglich gemäß Abs. 1 die Evidenzstellen (§ 49 Abs. 2) gemeinsam Verantwortliche im Sinne der DSGVO. Wie bereits nach bisheriger Rechtslage hat jede Evidenzstelle Zugriff auf den Gesamtbestand der im ZSR verarbeiteten Daten, unabhängig davon, welche Evidenzstelle die Daten im Register zur Verfügung gestellt hat.

Zu Art. 87 Z 5 (§ 56a Abs. 1a StbG):

Hinsichtlich der Erfüllung von Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstigen Pflichten nach den Bestimmungen der DSGVO sieht die Verordnung für gemeinsam Verantwortliche in

Art. 26 Abs. 1 Satz 2 vor, dass die Zuständigkeitsverteilung bezüglich der Wahrnehmung dieser Pflichten unter den Verantwortlichen in einer Vereinbarung festzulegen ist, sofern eine entsprechende Aufgabenverteilung unter den Verantwortlichen nicht bereits durch Rechtsvorschriften der Union oder der Mitgliedstaaten erfolgte. Vor diesem Hintergrund sieht der vorgeschlagene Abs. 1a vor, dass jeder Verantwortliche – dh. jede Evidenzstelle – die oa. Pflichten nur in Bezug auf jene Personen zu erfüllen hat, deren personenbezogenen Daten er selbst verarbeitet. Eine derartige Zuständigkeitsverteilung erscheint zweckmäßig, da jener Verantwortliche, der die personenbezogenen Daten des Betroffenen verarbeitet, am ehesten zu beurteilen vermag, ob ein derartiges Auskunfts-, Informations-, Berichtigungs-, Löschungs- oder sonstiges Begehren gerechtfertigt ist. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB. das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird. Nimmt ein Betroffener unter Nachweis seiner Identität ein Recht nach der DSGVO gegenüber einem unzuständigen Verantwortlichen wahr, ist er gemäß dem letzten Satz des neuen Abs. 1a an den zuständigen Verantwortlichen zu verweisen.

Zu Art. 87 Z 6 (§ 56a Abs. 2 StbG):

Durch die Änderungen in Abs. 2 wird den Vorgaben der DSGVO entsprochen. Beim Auftragsverarbeiter handelt es sich um einen Dritten, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Z 8 in Verbindung mit Art. 28 DSGVO). Als solcher entspricht er im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das ZSR bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig die Funktion des Auftragsverarbeiters zu übertragen. Darüber hinaus darf er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen.

Zur terminologischen Änderung im letzten Satz des Abs. 2 siehe die Erläuterungen zu §§ 39a Abs. 1 und 56b Abs. 4.

Zu Art. 87 Z 8 (§ 56b Abs. 6 StbG):

Es wird klargestellt, dass es sich bei der Abkürzung „ZPR“ um das in § 44 des Personenstandsgesetzes 2013 (PStG 2013) geregelte „Zentrale Personenstandsregister“ handelt.

Zu Art. 87 Z 9 (§ 56b Abs. 8 StbG):

Die DSGVO enthält keine Bestimmung über Protokollierungsvorschriften, innerstaatliche Regelungen sind daher zulässig. Da die Protokollierungsvorschriften des § 14 DSG 2000 entfallen, sind in jedem Materiengesetz gesonderte Protokollierungsvorschriften vorzusehen um ein gleichbleibendes Datenschutzniveau zu gewährleisten. Dies erfolgt im StbG durch den vorgeschlagenen § 56b Abs. 8.

Zu Art. 87 Z 10 (§ 64a Abs. 27 StbG):

Diese Bestimmung regelt das Inkrafttreten.

Zu Art. 87 Z 11 (§ 66 Abs. 1 lit. c StbG):

Hierbei handelt es sich lediglich um eine Verweisanpassung.

Artikel 88 (Änderung des Sicherheitspolizeigesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“).

Allgemeines:

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DS-RL sowie deren innerstaatliche Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes.

Der Begriff der „Verarbeitung“ personenbezogener Daten bedeutet gemäß § 36 Abs. 2 Z 2 DSG (bzw. Art. 3 Z 1 DS-RL) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die

Vernichtung. Indem die „Verarbeitung“ auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung beinhaltet, entspricht sie damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff der „Verwendung“ personenbezogener Daten. Zum anderen soll von diesem Begriff auch das „Ermitteln“ personenbezogener Daten als Unterfall des „Verarbeitens von Daten“ iSd § 4 Z 9 DSG 2000 erfasst sein, sodass der Begriff des „Verarbeitens“ nunmehr auch das Ermitteln und Weiterverarbeiten einbezieht, soweit die Erwähnung des Ermittelns im Sinne des Ermittlungsdienstes nicht explizit erforderlich erscheint.

Dem Begriff der „Datenanwendung“ (§ 4 Z 7 DSG 2000) entspricht nunmehr der Terminus der „Datenverarbeitung“.

Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 8 und § 47 DSG (bzw. der DS-RL gemäß Art. 3 Z 8 und 21 Abs. 1 DS-RL) der „Verantwortliche“ bzw. „gemeinsam Verantwortliche“ einer Datenverarbeitung.

Dem „Dienstleister“ (§ 4 Z 5 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 9 in Verbindung mit § 48 DSG (bzw. der DS-RL gemäß Art. 3 Z 9 in Verbindung mit Art. 22 DS-RL) der „Auftragsverarbeiter“. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser gemäß § 48 DSG nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des Datenschutzgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der „Auftragsverarbeiter“ im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000.

Dem DSG sowie der DS-RL sind der Begriff des „Informationsverbundsystems“ (bisher § 4 Z 13 DSG 2000) nicht mehr bekannt; dieser wird nunmehr durch die Datenverarbeitung durch „gemeinsam Verantwortliche“ (§ 47 DSG bzw. 21 Abs. 1 DS-RL) ersetzt. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen. Materielle Änderungen gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der gemeinsamen Datenverarbeitung verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall ursprünglich zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Zu Art. 88 Z 1 bis 7 (Inhaltsverzeichnis):

Es handelt sich um die erforderlichen Anpassungen des Inhaltsverzeichnisses.

Zu Art. 88 Z 8 (§ 7 Abs. 4 SPG):

Die vorgeschlagenen Änderungen dienen im Wesentlichen der Anpassung an die Vorgaben der unmittelbar anwendbaren DSGVO. Um die geistige und körperliche Eignung von Aufnahmewerbern in den Exekutivdienst und von Bewerbern für bestimmte Verwendungen beurteilen zu können, durften schon bislang – unter Einbindung von Polizeiärzten als medizinische Sachverständige – auch Gesundheitsdaten verarbeitet werden, soweit diese zur Beurteilung der Eignung für den Exekutivdienst erforderlich sind. Da es sich hierbei nicht um die Verarbeitung von Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung gemäß DS-RL handelt, unterfallen diese dem Rechtsschutzsystem der DSGVO.

Gesundheitsdaten sind nach der Definition des Art. 4 Z 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die Verarbeitung personenbezogener Daten ist im gegenständlichen Fall in Erfüllung des Art. 6 Abs. 1 lit. e DSGVO für die Wahrnehmung der im öffentlichen Interesse liegenden Aufgabe der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit durch körperlich und geistig geeignete Organe erforderlich. Da Gesundheitsdaten jedoch auch besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO darstellen, ist deren Verarbeitung nur bei Vorliegen bestimmter Fälle entsprechend Art. 9 Abs. 2 DSGVO zulässig. Die Verarbeitung der Gesundheitsdaten ist im gegebenen Zusammenhang für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich (Art. 9 Abs. 2 lit. h DSGVO). Die Verarbeitung zu diesem Zweck ist zulässig, da diese Daten entsprechend Art. 9 Abs. 3 DSGVO von Fachpersonal (oder unter dessen Verantwortung) verarbeitet werden, welches Berufsgeheimnispflichten unterliegt. Künftig ist deren Verarbeitung somit nach Maßgabe des Art. 9 Abs. 2 lit. h in Verbindung mit Abs. 3 DSGVO zulässig.

Im Übrigen handelt es sich um eine redaktionelle Bereinigung.

Zu Art. 88 9 und 10 (§ 13a SPG):

Die vorgeschlagenen Änderungen dienen hauptsächlich der terminologischen Anpassung an die DS-RL sowie deren innerstaatliche Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes.

Zu Abs. 3: Die Datensicherheit von Aufzeichnungen, die nach Abs. 3 zum Zwecke der Dokumentation von Amtshandlungen vorgenommen werden, erfolgte bislang nach den Bestimmungen des § 14 DSG 2000, welchem nunmehr im Wesentlichen § 54 DSG entspricht. Dieser verpflichtet den Verantwortlichen sowie den Auftragsverarbeiter dazu, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Da im Rahmen von Aufzeichnungen von Amtshandlungen jedoch auch personenbezogene Daten verarbeitet werden können, die nicht vom Zwecke der DS-RL und damit des 3. Hauptstücks des DSG erfasst sind – etwa bei Aufzeichnungen im Rahmen von Demonstrationen oder der Dokumentation von Handlungen der ersten allgemeinen Hilfeleistungspflicht –, unterliegen die Datensicherheitsmaßnahmen in solchen Fällen den Bestimmungen der unmittelbar zu Anwendung kommenden DSGVO.

Zu Abs. 4: Bislang erfolgte die Protokollierung von Dokumentationen iSd § 13a – insbesondere die Speicherdauer – nach den Vorgaben des § 14 DSG. Dieser sah in Abs. 5 eine generelle Aufbewahrungsfrist für Protokolldaten vor, sofern gesetzlich nicht ausdrücklich anderes angeordnet war. Eine solche Bestimmung findet sich jedoch nicht mehr im DSG, sodass mit dem vorgeschlagenen Abs. 4 eine solche Aufbewahrungsfrist von drei Jahren normiert wird.

Zu Art. 88 Z 11, 12, 14, 21, 22, 24 bis 26, 33 bis 37, 45, 46, 51, 53, 55, 58 und 61 bis 63 (§ 35a Abs. 5, Überschrift des 4. Teils, § 52, § 53b, § 54 Abs. 5, 6 und 7, § 55 Abs. 4, § 55a Abs. 4, § 55b Abs. 1, § 57, § 58, § 60 Abs. 2, § 61, § 67, § 69 Abs. 2, § 71 Abs. 5, § 75 Abs. 2, § 91c Abs. 2 und § 91d Abs. 3 SPG):

Es handelt sich um die Anpassung an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen.

Zu Art. 88 Z 13 (§ 51 SPG):

Die Änderungen dienen der Anpassung an die §§ 39 und 48 DSG.

Zu Abs. 1: Der Begriff der „sensiblen Daten“ gemäß § 4 Z 2 DSG 2000 wurde nunmehr durch den Begriff der „besonderen Kategorien personenbezogener Daten“ gemäß § 39 DSG (Art. 10 DS-RL) ersetzt. Hiervon erfasst sind personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung solcher Kategorien von Daten für die Zwecke des 3. Hauptstücks des DSG – und damit für Zwecke der Sicherheitspolizei – ist dann zulässig, wenn die Verarbeitung unbedingt erforderlich ist, wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und – sofern der Betroffene die Daten nicht offensichtlich selbst öffentlich gemacht hat – die Verarbeitung gesetzlich vorgesehen ist. Durch die Änderung des zweiten Satz des Abs. 1 soll das Erfordernis der Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen der Sicherheitspolizei erfüllt werden. Eine solche ist – entsprechend der datenschutzrechtlichen Vorgaben – zulässig, wenn dies zur Erfüllung der Aufgaben im Rahmen der Sicherheitspolizei unbedingt erforderlich ist; wie bislang sind angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Einer ausdrücklichen Anordnung, dass bei der Verarbeitung strafrechtlich relevanter Daten angemessene Vorkehrungen zur Wahrung ebendieser Interessen getroffen werden müssen, bedarf es künftig nicht. Handelt es sich um strafrechtlich relevante Daten, so geschieht die Verarbeitung im Rahmen des SPG regelmäßig auf Grundlage des 3. Hauptstücks des DSG bzw. der DS-RL, wodurch bereits besondere Maßnahmen bei der Datenverarbeitung vorgesehen sind.

Mit der Regelung des Abs. 1 zweiter Satz soll klargestellt sein, dass die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen der Aufgabenerfüllung der Sicherheitspolizei bei unbedingter Erforderlichkeit zulässig ist; es bedarf grundsätzlich keiner zusätzlichen ausdrücklichen Ermächtigungen. Soll die Verarbeitung solcher besonderen Daten jedoch nicht in jedem Fall – etwa nur zu bestimmten Zwecken oder nur bei bestimmten Kategorien – zulässig sein, wird dies durch ausdrückliche Erwähnung der besonderen Fälle deutlich gemacht. So ist etwa im Rahmen der Vertrauenspersonenevidenz gemäß § 54b die Verarbeitung besonderer Kategorien personenbezogener

Daten ausdrücklich nur zu den Zwecken zur Verhinderung von Gefährdungen der Betroffenen und zur Bewertung der Vertrauenswürdigkeit der Informationen zulässig. Demgegenüber sieht etwa § 53a Abs. 2 den Fall der Einschränkung auf bestimmte Kategorien vor, indem die Daten, die verarbeitet werden dürfen, taxativ genannt werden. Soweit bestimmte besondere Kategorien von den aufgezählten Datenarten erfasst sind, können diese auch im Rahmen des § 53a Abs. 2 verarbeitet werden – andere, nicht von der Aufzählung erfasste, besondere Kategorien hingegen nicht. Durch § 51 Abs. 1 zweiter Satz soll diese abschließende Aufzählung keine Erweiterung erfahren.

Sofern nicht ausdrücklich anderes angeordnet wird, finden auf das Verarbeiten personenbezogener Daten die Bestimmungen des Datenschutzgesetzes Anwendung. Die Anforderungen des § 43 Abs. 1 DSG werden insbesondere durch die gesetzliche Grundlage für die Datenverarbeitungen im SPG erfüllt.

Zu Abs. 3: Durch den neu vorgeschlagenen Abs. 3 soll im Allgemeinen normiert werden, dass die Rolle des Auftragsverarbeiters für alle Datenverarbeitungen nach dem SPG dem Bundesminister für Inneres zukommen soll; es ist jedoch möglich, gesonderte Regelungen vorzusehen. Der Auftragsverarbeiter im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem „Betreiber“ gemäß § 50 Abs. 1 DSG 2000. Damit kommt gemäß Abs. 3 die Funktion des Betreibers nunmehr ausdrücklich dem Bundesminister für Inneres in seiner Funktion als Auftragsverarbeiters zu, sofern nicht ausdrücklich anderes angeordnet wird.

§ 48 Abs. 2 DSG sieht vor, dass ein Auftragsverarbeiter keinen weiteren Auftragsverarbeiter in Anspruch nehmen kann, ohne eine vorherige gesonderte schriftliche Genehmigung des Verantwortlichen eingeholt zu haben. Diese Vorschrift ist jedoch enger als die unionsrechtlichen Vorgaben des Art. 22 Abs. 2 DS-RL, welche es dem Verantwortlichen ermöglicht, eine allgemeine schriftliche Genehmigung für die Inanspruchnahme weiterer Auftragsverarbeiter zu erteilen. Im diesem Fall hat der Auftragsverarbeiter den Verantwortlichen nur über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu unterrichten. Den unionsrechtlichen Vorgaben entsprechend soll abweichend von § 48 Abs. 2 DSG auch die Erteilung einer allgemeinen schriftlichen Genehmigung des Verantwortlichen ermöglicht werden. Aufgrund der verfassungsrechtlichen Weisungsbefugnis des Bundesministers für Inneres als oberste Sicherheitsbehörde ist es ausreichend, bei gemeinsamen Datenverarbeitungen mit dem Bundesminister für Inneres als gemeinsam Verantwortlichen diesen von beabsichtigten Änderungen iSd Abs. 3 letzter Satz zu unterrichten.

Zu Abs. 4: Die vorgeschlagene Neueinführung eines Abs. 4 dient der Umsetzung des § 47 DSG.

Bislang sah § 50 DSG 2000 die Möglichkeit vor, dass mehrere Auftraggeber gemeinsam ein Informationsverbundsystem betreiben und damit Daten gemeinsam verarbeiten können. Nunmehr normiert § 47 DSG die gemeinsame Verarbeitung, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Hierbei fungieren die Verantwortlichen als gemeinsam Verantwortliche, die ihre jeweiligen Aufgaben nach dem Datenschutzgesetz, insbesondere hinsichtlich der Wahrnehmung der Rechte Betroffener und wer welchen Informationspflichten gemäß § 43 DSG nachkommt, festzulegen haben. Nur sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich normiert sind, hat dies mittels Vereinbarung zu geschehen.

In diesem Sinne soll der vorgeschlagene Abs. 4 gesetzlich die Zuständigkeiten zwischen den gemeinsam Verantwortlichen von Datenverarbeitungen auf Grundlage des SPG dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach dem Datenschutzgesetz von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst ursprünglich verarbeiteten Daten stehen. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige gemeinsam Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach dem Datenschutzgesetz zukommt. Möchte ein Betroffener ein Recht nach dem Datenschutzgesetz wahrnehmen, hat er hiefür seine Identität nachzuweisen, um missbräuchliche oder unberechtigte Geltendmachung angeblicher Rechte hintanhalten zu können.

Nimmt ein Betroffener ein Recht gegenüber einem unzuständigen gemeinsam Verantwortlichen wahr – somit nicht gegenüber demjenigen, der seine Daten ursprünglich verarbeitet und damit in die gemeinsame Datenverarbeitung eingespeichert hat –, hat dieser durch Konsultation des zuständigen gemeinsam Verantwortlichen zu prüfen, ob die Unterrichtung des Betroffenen womöglich gemäß § 43 Abs. 4 aufgeschoben, eingeschränkt oder unterlassen werden soll. Liegt kein solcher Fall vor, ist der Betroffene gemäß dem letzten Satz des neuen Abs. 4 an den zuständigen gemeinsam Verantwortlichen zu verweisen.

Begehrt der Betroffene jedoch die Aktualisierung oder Richtigstellung von Namen, Geschlecht, früheren Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort, Wohnanschrift, Namen der Eltern oder

Aliasdaten gemäß § 59 Abs. 1 zweiter Satz, kann dies von jedem gemeinsam Verantwortlichen vorgenommen werden. Eine Verweisung auf denjenigen gemeinsam Verantwortlichen, der die Daten ursprünglich eingespeichert hat, ist in diesem Fall nicht erforderlich. Eine vorgenommene Berichtigung iSd § 59 Abs. 1 zweiter Satz bewirkt jedoch keine Änderung der Zuständigkeit des ursprünglichen gemeinsam Verantwortlichen. Werden in Folge weitere Ansprüche iSd DSG geltend gemacht, obliegt deren Wahrnehmung weiterhin dem ursprünglich gemeinsam Verantwortlichen, auch wenn zwischenzeitlich eine Berichtigung der Daten iSd § 59 Abs. 1 zweiter Satz von einer anderen Sicherheitsbehörde vorgenommen wurde.

Zu Art. 88 Z 15 (§ 53 SPG):

Es handelt sich um begriffliche Anpassungen an das DSG und redaktionelle Bereinigungen. Der Begriff des „Ermittelns“ soll nunmehr vom Terminus des „Verarbeitens“ erfasst sein, sodass es keiner getrennten Erwähnung von „Ermitteln“ und „(Weiter-)Verarbeiten“ bedarf und dennoch die materielle Rechtslage beibehalten wird.

Zu Art. 88 Z 16 bis 20 (§ 53a SPG):

Die Änderungen dienen im Wesentlichen der begrifflichen Anpassung an das DSG.

Zu Abs. 2: Da bereits § 51 Abs. 1 eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten im Rahmen der Sicherheitspolizei normiert, bedarf es grundsätzlich keiner weiteren Anführung. Die Verarbeitung ist dabei natürlich an die Grenzen und Erfordernisse des § 39 DSG sowie des § 51 Abs. 1 gebunden, sodass diese nur bei unbedingter Erforderlichkeit zulässig ist. Demgegenüber sieht etwa § 53a Abs. 2 den Fall der Einschränkung auf bestimmte Kategorien vor, indem die Daten, die verarbeitet werden dürfen, taxativ genannt werden. Soweit bestimmte besondere Kategorien von den aufgezählten Datenarten erfasst sind, können diese auch im Rahmen des § 53a Abs. 2 verarbeitet werden – andere, nicht von der Aufzählung erfasste, besondere Kategorien hingegen nicht. Durch § 51 Abs. 1 zweiter Satz soll diese abschließende Aufzählung keine Erweiterung erfahren.

Zu Abs. 5 bis 6: Die sonstigen vorgeschlagenen Änderungen der Abs. 5 bis 6 dienen – ohne eine materielle Änderung der Rechtslage herbeizuführen – lediglich einer sprachlichen Vereinfachung.

Der Auftragsverarbeiter im Sinne des § 36 Abs. 2 Z 9 DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Die Funktion des Betreibers übte in Bezug auf die zentrale Datenverarbeitung nach Abs. 5a bisher ausdrücklich das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung aus. Nunmehr weist § 51 Abs. 3 erster Satz dem Bundesminister für Inneres die Funktion des Auftragsverarbeiters zu, sofern nicht ausdrücklich anderes angeordnet wird. Da das Bundesamt jedoch eine Organisationseinheit der Sicherheitsbehörde Bundesminister für Inneres ist (vgl. § 1 Abs. 3 Polizeiliches Staatsschutzgesetz in Verbindung mit § 6 Abs. 1) und damit im Innenverhältnis auch weiterhin mit der faktischen Aufgabe der Auftragsverarbeitung betraut werden kann, bedarf es keiner von der Generalklausel des § 51 Abs. 3 erster Satz abweichenden Regelung. Wenngleich nunmehr das Bundesamt nicht mehr ausdrücklich in Abs. 5a angeführt wird, wird damit keine tatsächliche Änderung des aktuellen Rechtsbestands herbeigeführt.

Zu Art. 88 Z 23 (§ 54b Abs. 1 und 3 SPG):

Es handelt sich in erster Linie um eine terminologische Anpassung an die neuen Begrifflichkeiten des DSG. Wie bereits geltend soll auch weiterhin klargestellt sein, dass besondere Kategorien personenbezogener Daten nur soweit verarbeitet werden dürfen, als dies zur Verhinderung von Gefährdungen der Betroffenen und zur Bewertung der Vertrauenswürdigkeit der Informationen unbedingt erforderlich ist. § 51 Abs. 1 zweiter Satz soll diese Zweckbeschränkung nicht erweitern.

Da strafrechtsbezogene Daten künftig keinem gesonderten Regime unterliegen und auch nicht vom Begriff der besonderen Kategorien von Daten erfasst sind, sind diese als personenbezogene Daten zu verarbeiten.

Jede Verarbeitung der in der Vertrauenspersonenevidenz verarbeiteten personenbezogenen Daten ist – auch weiterhin – zu protokollieren. Da die Protokollierung für Datenverarbeitungen im Rahmen der Sicherheitspolizei nach dem 4. Teil des SPG nunmehr generell in § 63 Abs. 3 normiert ist, bedarf es keiner gesonderten Bestimmung in § 54b Abs. 3, sodass diese zu entfallen hat. Die Protokollierung erfolgt künftig auf Grundlage des § 63 Abs. 3.

Zu Art. 88 Z 27 bis 32 (§ 56 SPG):

Die Änderungen des Abs. 1 dienen der Anpassung an das DSG, wobei Z 1 lediglich begrifflicher Natur ist.

Zu Abs. 1: Die Übermittlung personenbezogener Daten – unabhängig davon, ob es sich auch um besondere Kategorien personenbezogener Daten handelt – zur Wahrung lebenswichtiger Interessen einer Person bedarf entsprechend § 38 DSG keiner ausdrücklichen Rechtsgrundlage mehr. Wenngleich eine Übermittlung zu diesem Zweck nunmehr auch ohne gesetzliche Regelung zulässig ist, soll Abs. 1 Z 5 zur Vermeidung von Rechtsunsicherheiten grundsätzlich beibehalten werden. Da die Übermittlung jedoch generell zulässig ist, unabhängig von der Einordnung des zu übermittelnden Datums als besondere Kategorie, hat der Halbsatz zu den vormals sensiblen Daten zu entfallen.

Die Übermittlung gemäß Abs. 1 Z 7 für Zwecke der wissenschaftlichen Forschung und Statistik ist im Anwendungsbereich des § 36 Abs. 1 DSG – somit insbesondere für Zwecke der Sicherheitspolizei – nach den Bestimmungen des DSG zulässig, im Anwendungsbereich der DSGVO nach den unmittelbar geltenden Bestimmungen dieser. Der Verweis auf die Regelung des § 46 DSG 2000 hat zu entfallen.

Im Übrigen handelt es sich um eine redaktionelle Ergänzung.

Zu Abs. 2: Die Regelungen zur Protokollierung finden sich nunmehr gebündelt in § 63 Abs. 3, sodass Abs. 2 zu entfallen hat. Auch die Bestimmung hinsichtlich automatisierter Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt. Damit bleibt das hohe Niveau des Datenschutzes für Personen, deren KFZ-Kennzeichen zwar durch Kennzeichenerkennungsgeräte erfasst wurden ohne einen Trefferfall zu bewirken, auch weiterhin aufrecht.

Zu Abs. 3: Abs. 3 regelte bislang die Vorgehensweise bei der Übermittlung von unvollständigen oder unrichtigen Daten; dies ist nunmehr insbesondere § 37 DSG zu entnehmen. Gemäß § 37 Abs. 6 DSG dürfen unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten nicht übermittelt werden. Zu diesem Zweck sind die Daten vor einer Übermittlung soweit möglich entsprechend zu überprüfen. Wird festgestellt, dass personenbezogene Daten übermittelt worden sind, die nicht diesen Anforderungen entsprechen, ist dies dem Empfänger unverzüglich mitzuteilen. Letzterer hat unverzüglich die Löschung unrechtmäßig übermittelter Daten, die Berichtigung unrichtiger Daten, die Ergänzung unvollständiger Daten oder eine Einschränkung der Verarbeitung vorzunehmen (§ 37 Abs. 8 DSG). Hat im umgekehrten Fall der Empfänger Grund zur Annahme, dass übermittelte personenbezogene Daten unrichtig, nicht aktuell oder zu löschen sind, ist dies dem Übermittler mitzuteilen, welcher unverzüglich die erforderlichen Maßnahmen zu setzen hat (§ 37 Abs. 9 DSG). Wenngleich diese Bestimmungen des DSG auch unmittelbar im Rahmen des SPG zur Anwendung kommen, wird im Sinne der Rechtssicherheit und Verständlichkeit des Gesetzes ein Verweis auf § 37 Abs. 8 und 9 DSG aufgenommen.

Zu Abs. 5: Insbesondere zum Zweck der Vermeidung zukünftiger Ausschreitungen bei Sportgroßveranstaltung ermöglicht Abs. 1 Z 3a die Übermittlung bestimmter personenbezogener Daten an den Österreichischen Fußballbund sowie die Österreichische Fußball-Bundesliga zur Prüfung und Veranlassung eines Sportstättenbetretungsverbotes. Abs. 5 sieht vor, dass eine solche Übermittlung nach Eingehen vertraglicher Verpflichtungen des Österreichischen Fußballbundes und der Österreichischen Fußball-Bundesliga zur Einhaltung bestimmter Sicherheitsmaßnahmen zulässig ist. Die Verarbeitung der übermittelten personenbezogenen Daten durch Fußballbund und Bundesliga erfolgt nicht zu einem Zweck des 3. Hauptstücks des DSG, sodass die Bestimmungen der DSGVO unmittelbar zur Anwendung kommen. Die Änderungen des Abs. 5 dienen im Übrigen der terminologischen Anpassung an die Begrifflichkeiten der DSGVO.

Zu Art. 88 Z 38 bis 42 (§ 58a, § 58b Abs. 1, § 58c, § 58d Abs. 1, § 58e SPG samt Überschrift):

Es handelt sich ausschließlich um Anpassungen an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen. Gemäß § 51 Abs. 3 kommt die Funktion des Betreibers dem Bundesminister für Inneres in seiner Funktion als Auftragsverarbeiters zu.

Zu Art. 88 Z 40 (§ 58c SPG):

Im Übrigen wurden redaktionelle Bereinigungen vorgenommen.

Zu Art. 88 Z 41 (§ 58d Abs. 1 SPG):

Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt entsprechend § 51 Abs. 1 zweiter Satz.

Zu Art. 88 Z 43, 43a und 44 (§ 59 SPG samt Überschrift):

Die Änderungen der Überschrift, des Abs. 1 und 3 dienen in erster Linie der begrifflichen Anpassung an das DSG.

In Konkretisierung des § 50 DSG finden sich die Regelungen zur Protokollierung nunmehr gebündelt in § 63 Abs. 3 für alle Datenverarbeitungen, unabhängig davon ob sie lokal oder zentral geführt werden, sodass Abs. 2 zu entfallen hat. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Die Zuordnung zu einem bestimmten Organwalter ist bei ausschließlich programmgesteuerten (vormalige Diktion: automatisierten) Abfragen auch weiterhin nicht erforderlich (vgl. Art. 25 Abs. 1 DS-RL, wonach die Identifizierung der Person, welche die Daten abgefragt oder offengelegt hat, nur so weit wie möglich zu ermöglichen ist). Von der Protokollierung ausgenommen bleiben automatisierte Abfragen gemäß § 54 Abs. 4b, es sei denn, es handelt sich um einen Trefferfall. Auch die Bestimmung hinsichtlich automatisierter Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr in § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt.

Zu Art. 88 Z 47 (§ 63 SPG samt Überschrift):

Die Änderungen der Überschrift und des Abs. 1 dienen der Anpassung an das DSG.

Die Regelungen zur Protokollierung iSd § 50 DSG finden sich nunmehr gebündelt in einem neuen Abs. 3 für alle Datenverarbeitungen, unabhängig davon ob sie lokal oder zentral geführt werden, wobei festzuhalten ist, dass die Verarbeitung von Daten innerhalb der Organisationsstruktur des Verantwortlichen bzw. durch gemeinsam Verantwortliche keine Übermittlung iSd § 50 DSG darstellt. Die vormalige Regelung des § 59 Abs. 2 wurde übernommen, indem die Zuordnung zu einem bestimmten Organwalter bei ausschließlich programmgesteuerten (vormalige Diktion: automatisierten) Abfragen auch weiterhin nicht erforderlich ist (vgl. Art. 25 Abs. 1 DS-RL, wonach die Identifizierung der Person, welche die Daten abgefragt oder offengelegt hat, nur so weit wie möglich erforderlich ist, sowie § 59 Abs. 2 alt). Erfasst von dieser Ausnahmebestimmung sind solche Abfragen, die nicht durch eine Willensbetätigung eines Menschen initiiert werden, sondern ausschließlich durch ein Computersystem aufgrund seiner Programmierung vollautomatisch durchgeführt werden. Hierbei ist die Zuordnung zu einem bestimmten Organwalter nicht möglich, da kein Organ, sondern ausschließlich ein Computersystem, tätig wird. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Auch die Bestimmung hinsichtlich der ausschließlich programmgesteuerten (vormalige Diktion: automatisierter) Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr in § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt.

Zu Art. 88 Z 48 (§ 64 Abs. 2 SPG):

Die Änderungen dienen der Anpassung an die Bestimmungen des § 36 Abs. 2 Z 12 und 13 DSG.

§ 36 Abs. 2 Z 12 DSG definiert „genetische Daten“ als personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden; Z 13 beschreibt „biometrische Daten“ als mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten. Von diesen Begriffen erfasst sind etwa erkennungsdienstliche Maßnahmen wie die Abnahme von Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, die Herstellung von Abbildungen, die Vornahme von Messungen oder die Erhebung von Stimmproben.

Die neue Terminologie des DSG aufgreifend wird die Definition der „erkennungsdienstlichen Maßnahmen“ iSd SPG als technische Verfahren zur Feststellung von biometrischen oder genetischen Daten (§ 36 Abs. 2 Z 12 und 13 DSG) sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung aktualisiert. Eine materielle Änderung der bestehenden Rechtslage erfolgt durch die Neutextierung jedoch nicht.

Zu Art. 88 Z 49 und 50 (§ 65 SPG):

Die Änderung des Abs. 2 erfolgt in Anpassung an die Voraussetzungen des Abs. 1.

Da sich die Informations- und Verständigungspflichten unmittelbar insbesondere aus § 43 DSG ergeben, hat Abs. 5 keinen originären Anwendungsbereich und damit zu entfallen. Der Betroffene ist nunmehr nach den Bestimmungen des DSG (§§ 42 ff DSG) über seine Rechte zu informieren.

Im Übrigen handelt es sich um erforderliche begriffliche Anpassungen an das DSG.

Zu Art. 88 Z 52 (§ 68 SPG samt Überschrift):

Es handelt sich im Wesentlichen um Anpassungen an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen, sowie um sprachliche Vereinfachungen. Gemäß den Abs. 3 und 4 können Sicherheitsbehörden von Personen, die befürchten, Opfer eines Verbrechens bzw. eines Unfalles zu werden, mit deren Einwilligung erkennungsdienstliche Daten ermitteln, um

gefährlichen Angriffen gegen Leben oder Gesundheit vorzubeugen bzw. die Identifizierung eines Leichnams zu erleichtern. Bislang konnten diese Daten nur lokal bei der ermittelnden Sicherheitsbehörde gespeichert werden. Um im Anlassfall jedoch tatsächlich die Erfüllung des Speicherzwecks der Gefahrenvorbeugung bzw. Identifizierung unabhängig vom Ort der Gefahr oder des Unfalls sicherstellen zu können, bedarf es einer zentralen Datenverarbeitung. Daher sollen – wie bereits in Abs. 1 vorgesehen – auch die gemäß § 68 Abs. 3 und 4 ermittelten erkennungsdienstlichen Daten mit Einwilligung des Betroffenen in der Zentralen erkennungsdienstlichen Evidenz (§ 75) verarbeitet werden können.

Zu Art. 88 Z 54 (§ 70 SPG samt Überschrift):

Neben § 75 zur Zentralen erkennungsdienstlichen Evidenz traf § 70 Bestimmungen zur Aufbewahrung erkennungsdienstlicher Daten in lokal geführten erkennungsdienstlichen Evidenzen. Damit war es grundsätzlich jeder Sicherheitsbehörde ermöglicht, solche erkennungsdienstlichen Daten, die sie im Rahmen einer erkennungsdienstlichen Behandlung oder Maßnahme ermittelt hat, in einer lokalen Datenbank aufzubewahren. Darüber hinaus konnte der Bundesminister für Inneres durch Verordnung die Grundlage für regionale oder überregionale Evidenzen spezieller Daten nach Abs. 2 schaffen. Da diese Rechtsgrundlagen nach den Abs. 1 bis 3 jedoch über keine praktische Relevanz mehr verfügen, sollen diese bereinigt werden.

Abs. 4 hingegen ermöglicht es, Daten, die von Organen der Sicherheitsbehörden als „Gelegenheitspersonen“ – somit insbesondere von Kriminalbeamten, die regelmäßig mit der Klärung von Umständen gerichtlich strafbarer Handlungen am Tatort befasst sind – ermittelt wurden, in einer gesonderten Evidenz zu führen. Ziel dieser „Police-Elimination-Datei“ ist die Ausscheidung der von erkennungsdienstlich tätigen Beamten hinterlassenen Spuren bei der Tataufklärung. Diese Bestimmung steht im Zusammenhang mit § 65 Abs. 2 und § 67 Abs. 1 und erlaubt eine solche Datenermittlung bloß in Einzelfällen. § 70 soll nunmehr ausschließlich die Grundlage zur Führung einer solchen Police-Elimination-Datei, somit einer „Spurenausscheidungsevidenz“ sein. Die Führung dieser Evidenz obliegt dem Bundesminister für Inneres als Verantwortlichen. Im Übrigen handelt es sich lediglich um terminologische Anpassungen, insbesondere auch an das DSG sowie die Begrifflichkeit der §§ 65 und 67, und die Berichtigung eines redaktionellen Versehens.

Zu Art. 88 Z 56 (§ 73 Abs. 1 Z 5 SPG):

Die Änderung dient der Anpassung an die Überarbeitung des § 70.

Zu Art. 88 Z 57 (§ 75 Abs. 1 SPG):

Die Adaptierungen des Abs. 1 dienen der Anpassung an die Änderungen des § 68, der terminologischen Aktualisierung im Sinne des DSG sowie der sprachlichen Vereinfachung. Künftig können auch Daten, die gemäß § 68 Abs. 3 und 4 zum Zwecke der Vorbeugung gefährlicher Angriffe gegen Leben oder Gesundheit bzw. der Identifizierung von Toten mit Einwilligung des Betroffenen ermittelt wurden, in der Zentralen erkennungsdienstlichen Evidenz verarbeitet werden.

Zu Art. 88 Z 59 (§ 76 SPG):

Die Änderungen der Abs. 1, 2, 3 und 6 dienen der Anpassung an die Terminologie und Vorgaben des DSG sowie der redaktionellen Bereinigung. Die Änderungen des Abs. 4 erfolgen in Anpassung an die Überarbeitung des § 70.

Zu Art. 88 Z 60 (§ 80 SPG):

Die Änderungen gründen sich auf die Vorgaben des DSG. Indem Informationen gemäß § 43 DSG sowie alle Mitteilungen und Maßnahmen gemäß den §§ 44 und 45 DSG künftig unentgeltlich zur Verfügung zu stellen sind, hat Abs. 1 zu entfallen und ist Abs. 2 anzupassen. Im Übrigen handelt es sich um Anpassung an die Terminologie und die Bestimmungen des DSG.

Zu Art. 88 Z 61 (§ 90 SPG):

Die Änderung dient der Anpassung an die Vorgaben des DSG, wobei das bisher bestehende Regime nicht abgeändert werden soll. Zur Verarbeitung personenbezogener Daten zählt auch das Erheben, weshalb das „Ermitteln“ personenbezogener Daten prinzipiell von § 90 erfasst ist. Dies gilt allerdings auch weiterhin dann nicht, wenn die Ermittlung personenbezogener Daten in Form von verwaltungsbehördlicher Befehls- und Zwangsgewalt, etwa im Rahmen einer zwangsweisen Durchsuchung von Räumen, der zwangsunterstützten Anfertigung von Lichtbildern oder durch zwangsweise Erhebung anderer erkennungsdienstlicher Daten erfolgt. In diesen Fällen, in denen es um die Rechtmäßigkeit der Befugnisausübung geht, sollen – wie auch bisher – ausschließlich die Landesverwaltungsgerichte zur Entscheidung nach § 88 Abs. 1 zuständig sein.

Zu Art. 88 Z 64 (§ 94 Abs. 44 SPG):

Es handelt sich um die erforderlichen Inkrafttretens- und Außerkrafttretensbestimmungen.

Artikel 89 (Änderung des Polizeilichen Staatsschutzgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit").

Allgemeines:

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DS-RL sowie deren innerstaatliche Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes.

Der Begriff der „Verarbeitung" personenbezogener Daten bedeutet gemäß § 36 Abs. 2 Z 2 DSG (bzw. Art. 3 Z 1 DS-RL) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Indem die „Verarbeitung" auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung beinhaltet, entspricht sie damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff der „Verwendung" personenbezogener Daten. Zum anderen soll von diesem Begriff auch das „Ermitteln" personenbezogener Daten als Unterfall des „Verarbeitens von Daten" iSd § 4 Z 9 DSG 2000 erfasst sein, sodass der Begriff des „Verarbeitens" nunmehr auch das Ermitteln und Weiterverarbeiten einbezieht, soweit die Erwähnung des Ermittelns im Sinne des Ermittlungsdienstes nicht explizit erforderlich erscheint.

Dem Begriff der „Datenanwendung" (§ 4 Z 7 DSG 2000) entspricht nunmehr der Terminus der „Datenverarbeitung".

Dem „Auftraggeber" einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 8 und § 47 DSG (bzw. der DS-RL gemäß Art. 3 Z 8 und 21 Abs. 1 DS-RL) der „Verantwortliche" bzw. „gemeinsam Verantwortliche" einer Datenverarbeitung.

Dem „Dienstleister" (§ 4 Z 5 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 9 in Verbindung mit § 48 DSG (bzw. der DS-RL gemäß Art. 3 Z 9 DS-RL) der „Auftragsverarbeiter". Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser gemäß § 48 DSG nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des Datenschutzgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der „Auftragsverarbeiter" im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister" gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000.

Dem DSG sowie der DS-RL sind der Begriff des „Informationsverbundsystems" (bisher § 4 Z 13 DSG 2000) nicht mehr bekannt; dieser wird nunmehr durch die Datenverarbeitung durch „gemeinsam Verantwortliche" (§ 47 DSG bzw. 21 Abs. 1 DS-RL) ersetzt. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen. Materielle Änderungen gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der gemeinsamen Datenverarbeitung verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall ursprünglich zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Zu Art. 89 Z 1 (Überschrift des 3. Hauptstücks):

Es handelt sich um die erforderliche begriffliche Anpassung an das DSG.

Zu Art. 89 Z 2, 3 und 4 (§ 9 PStSG):

Die Änderungen dienen der Anpassung an das DSG, insbesondere an die §§ 36 Abs. 2 Z 2, 39 und 50 DSG. Die Anforderungen des § 43 Abs. 1 DSG werden insbesondere durch die gesetzliche Grundlage für die Datenverarbeitungen im PStSG erfüllt.

Der Begriff der „sensiblen Daten" gemäß § 4 Z 2 DSG 2000 wurde nunmehr durch den Begriff der „besonderen Kategorien personenbezogener Daten" gemäß § 39 DSG (Art. 10 DS-RL) ersetzt. Hiervon erfasst sind personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit

hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung solcher Kategorien von Daten für die Zwecke des 3. Hauptstücks des DSG – und damit für Zwecke des polizeilichen Staatsschutzes – ist dann zulässig, wenn die Verarbeitung unbedingt erforderlich ist, wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und – sofern der Betroffene die Daten nicht offensichtlich selbst öffentlich gemacht hat – die Verarbeitung gesetzlich vorgesehen ist. Durch die Änderung des zweiten Satz des Abs. 1 soll das Erfordernis der Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen des polizeilichen Staatsschutzes erfüllt werden. Eine solche ist – entsprechend der datenschutzrechtlichen Vorgaben – zulässig, wenn dies zur Erfüllung der Aufgaben nach dem PStSG unbedingt erforderlich ist; wie bislang sind angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Mit der Regelung des Abs. 1 zweiter Satz soll klargestellt sein, dass die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen der Aufgabenerfüllung nach dem PStSG – wie bisher – bei unbedingter Erforderlichkeit zulässig ist; es bedarf grundsätzlich keiner zusätzlichen ausdrücklichen Ermächtigungen. Soll die Verarbeitung solcher besonderen Daten jedoch nicht in jedem Fall – etwa nur zu bestimmten Zwecken oder nur bei bestimmten Kategorien – zulässig sein, wird dies durch ausdrückliche Erwähnung der besonderen Fälle deutlich gemacht.

In § 50 DSG finden sich die Regelungen zur Protokollierung für alle Datenverarbeitungen. Demnach sind über jeden Verarbeitungsvorgang Protokollaufzeichnungen zu führen, aus denen zumindest Zweck, Datum und Uhrzeit des Vorgangs, die Identität der Person, die die Daten verarbeitet hat, sowie allfällige Übermittlungsempfänger ersichtlich sind. Bei der Verarbeitung von Daten innerhalb der Organisationsstruktur des Verantwortlichen bzw. durch gemeinsam Verantwortliche handelt es sich nicht um eine Übermittlung in diesem Sinne. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.

Gemäß § 43 Abs. 4 DSG kann aus bestimmten Gründen die Information des Betroffenen über seine Person betreffende Datenverarbeitungen aufgeschoben, eingeschränkt oder unterlassen werden. Dies gilt gemäß § 44 Abs. 2 und 3 DSG auch ausdrücklich im Zusammenhang mit dem Auskunftsrecht Betroffener. Gemäß Art. 16 DS-RL kann gesetzlich eine solche Beschränkung ebenso hinsichtlich des Rechts auf Berichtigung oder Löschung bzw. auf Einschränkung der Verarbeitung vorgesehen werden. Durch den neuen Abs. 4 soll – in Entsprechung des Art. 16 DS-RL – bei Vorliegen der Voraussetzungen des § 43 Abs. 4 DSG auch in Fällen des § 45 Abs. 4 DSG von der Unterrichtung des Betroffenen Abstand genommen werden können.

Zu Art. 89 Z 5 und 6 (§ 10 PStSG):

Da bereits § 9 Abs. 1 eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten im Rahmen polizeilichen Staatsschutzes normiert, bedarf es grundsätzlich keiner weiteren Anführung. Die Verarbeitung ist dabei natürlich an die Grenzen und Erfordernisse des § 39 DSG sowie des § 9 Abs. 1 gebunden, sodass diese nur bei unbedingter Erforderlichkeit zulässig ist.

Im Übrigen handelt es sich um begriffliche Anpassungen an das DSG, ohne eine Änderung der materiellen Rechtslage herbeizuführen. Der Begriff des „Ermittelns“ soll nunmehr vom Terminus des „Verarbeitens“ erfasst sein, sodass es keiner getrennten Erwähnung von „Ermitteln“ und „Verarbeiten“ bedarf und dennoch die materielle Rechtslage beibehalten wird.

Zu Art. 89 Z 7, 8, 9, 10 und 11(§ 12 PStSG):

Die vorgeschlagenen Änderungen erfolgen in Anpassung an das DSG, insbesondere in Umsetzung der §§ 47 f DSG.

Der Begriff des „Informationsverbundsystems“ (bisher § 4 Z 13 DSG 2000) wird nunmehr durch die Datenverarbeitung durch „gemeinsam Verantwortliche“ (§ 47 DSG bzw. 21 Abs. 1 DS-RL) ersetzt. Gemäß § 48 Abs. 1 DSG kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet („Auftragsverarbeiter“ iSd § 36 Abs. 2 Z 9 DSG). Der Auftragsverarbeiter im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem „Betreiber“ gemäß § 50 Abs. 1 DSG 2000. Die Funktion des Betreibers in Bezug auf Datenverarbeitungen nach § 12 übte bisher ausdrücklich das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung aus. Nunmehr soll gemäß Abs. 1 letzter Satz die Rolle des „Auftragsverarbeiters“ dem Bundesminister für Inneres zukommen. Als eine Organisationseinheit der Sicherheitsbehörde Bundesminister für Inneres (vgl. § 1 Abs. 3 in Verbindung mit § 6 Abs. 1 SPG) ist das Bundesamt im Innenverhältnis auch weiterhin mit der faktischen Aufgabe der Auftragsverarbeitung

betraut. Wenngleich nunmehr das Bundesamt nicht mehr ausdrücklich angeführt wird, wird damit keine tatsächliche Änderung des aktuellen Rechtsbestands herbeigeführt.

Bislang sah § 50 DSG 2000 die Möglichkeit vor, dass mehrere Auftraggeber gemeinsam ein Informationsverbundsystem betreiben und damit Daten gemeinsam verarbeiten können. Nunmehr normiert § 47 DSG die gemeinsame Verarbeitung, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Hierbei fungieren die Verantwortlichen als gemeinsam Verantwortliche, die ihre jeweiligen Aufgaben nach dem Datenschutzgesetz, insbesondere hinsichtlich der Wahrnehmung der Rechte Betroffener und wer welchen Informationspflichten gemäß § 43 DSG nachkommt, festzulegen haben. Nur sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich normiert sind, hat dies mittels Vereinbarung zu geschehen. In diesem Sinne soll der vorgeschlagene Abs. 5 gesetzlich die Zuständigkeiten zwischen den gemeinsam Verantwortlichen von Datenverarbeitungen auf Grundlage des PStSG dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach dem Datenschutzgesetz von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst ursprünglich verarbeiteten Daten stehen. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige gemeinsam Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach dem Datenschutzgesetz zukommt. Möchte ein Betroffener ein Recht nach dem Datenschutzgesetz wahrnehmen, hat er seine Identität nachzuweisen, um missbräuchliche oder unberechtigte Geltendmachung angeblicher Rechte hintanhalten zu können. Nimmt ein Betroffener jedoch ein Recht gegenüber einem unzuständigen gemeinsam Verantwortlichen wahr – somit nicht gegenüber demjenigen, der seine Daten ursprünglich verarbeitet und damit in die gemeinsame Datenverarbeitung eingespeichert hat –, hat dieser durch Konsultation des zuständigen gemeinsam Verantwortlichen zu prüfen, ob die Unterrichtung des Betroffenen womöglich gemäß § 43 Abs. 4 aufgeschoben, eingeschränkt oder unterlassen werden soll. Liegt kein solcher Fall vor, ist der Betroffene gemäß dem letzten Satz des neuen Abs. 8 an den zuständigen gemeinsam Verantwortlichen zu verweisen. Im Übrigen handelt es sich um die erforderlichen begrifflichen Anpassungen an das DSG.

Zu Art. 89 Z 12, 13 und 14 (§§ 13, 14 Abs. 1 und 15 Abs. 1 PStSG):

Es handelt sich ausschließlich um Anpassungen an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen.

Zu Art. 89 Z 15 und 16 (§ 16 Abs. 1 und 3 PStSG):

Es handelt sich um die begriffliche Anpassung an das DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen.

Zu Art. 89 Z 17 (§ 18 Abs. 3 PStSG):

Es handelt sich um die erforderliche Inkrafttretensbestimmung.

Artikel 90 (Änderung des Polizeikooperationsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“).

Zu Art. 90 Z 1 und 2 (Inhaltsverzeichnis):

Die Änderungen stellen notwendige Adaptierungen des Inhaltsverzeichnisses dar.

Zu Art. 90 Z 3, 4, 5, 7 und 18 (§ 3 Abs. 2 Z 1, § 5 Abs. 1 Z 2 und Abs. 3 Z 1, § 7 Abs. 1 und 5, § 18 Z 1 PolKG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die datenschutzrechtlichen Vorgaben der DSGVO sowie der DS-RL und deren innerstaatlichen Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes.

Der Begriff „Verarbeitung“ wird in § 36 Abs. 2 Z 2 DSG (Art. 3 Z 2 DS-RL) als jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten definiert. Dies umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Eine Differenzierung zwischen den Begriffen „Ermitteln“, „Verwenden“ und „Verarbeiten“

besteht nicht mehr und es werden alle gänzlich von „Verarbeiten“ erfasst. Im Sinne der Klarstellung wird jedoch vereinzelt von der Verwendung des umfassenden Begriffs „Verarbeiten“ abgegangen und lediglich von „Ermitteln“ oder „Übermitteln“ gesprochen, um die im jeweiligen Kontext konkret zulässige Form des „Verarbeitens“ klar zu definieren. Auch ist die Verwendung des Begriffs „Ermitteln“ dem DSG zu entnehmen.

Dem bisherigen Begriff des „Auftraggebers“ entspricht nunmehr die Definition des „Verantwortlichen“ (§ 36 Abs. 2 Z 8 DSG, Art. 3 Z 8 DS-RL) und wird damit die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, definiert. Dem bisherigen Begriff des „Dienstleisters“ entspricht nunmehr die Definition des „Auftragsverarbeiters“ (§ 36 Abs. 2 Z 9 DSG, Art. 3 Z 9 DS-RL), der als natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, definiert wird.

Dem Begriff der „Datenanwendung“ (§ 4 Z 7 DSG 2000) entspricht nunmehr der Terminus der „Datenverarbeitung“.

Das rechtliche Konstrukt des Informationsverbundsystems des bisherigen § 50 DSG 2000 ist dem neuen datenschutzrechtlichen System in dieser Form nicht bekannt. Dieses wird künftig durch eine Datenverarbeitung von zwei oder mehr Verantwortlichen, die gemeinsam den Zweck und die Mittel einer Datenverarbeitung festlegen, dargestellt. In diesem Konstrukt treffen grundsätzlich alle Verantwortlichen die entsprechenden Pflichten der Wahrnehmung der Rechte der betroffenen Person gleichermaßen, insbesondere Informations- und Auskunftspflichten. Die jeweiligen Aufgaben können jedoch gemäß § 47 DSG (Art. 21 Abs. 1 DS-RL) gesetzlich festgelegt werden.

Zu Art. 90 Z 6 (§ 8 PolKG):

Die DSGVO differenziert hinsichtlich des Zwecks der Verarbeitung personenbezogener Daten. Dient die Verarbeitung personenbezogener Daten dem Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sind die Bestimmungen der DS-RL anzuwenden, welche im 3. Hauptstück des DSG innerstaatlich umgesetzt wurde. Erfolgt die Verarbeitung personenbezogener Daten zu anderen als diesen Zwecken, sind die jeweiligen Bestimmungen der DSGVO einschlägig. Da das PolKG gemäß § 1 Abs. 1 die internationale polizeiliche Kooperation sowohl zu Zwecken der Sicherheits- und Kriminalpolizei (und somit im Anwendungsbereich der DS-RL bzw. dem 3. Hauptstück des DSG) als auch zu Zwecken des Passwesens, der Fremdenpolizei und der Grenzkontrolle (die dem Regime der DSGVO unterliegen) regelt, muss dies hinsichtlich der Zulässigkeit der Übermittlung berücksichtigt werden.

Da sowohl die DSGVO als auch die DS-RL bzw. das DSG weiters hinsichtlich der Übermittlung personenbezogener Daten an Mitgliedstaaten und an Drittstaaten sowie internationale Organisationen differenziert, muss hierauf ebenso Bedacht genommen werden.

Folglich ist im Anwendungsbereich des PolKG einerseits zwischen Übermittlungen zum Zweck der Sicherheits- und Kriminalpolizei und sonstigen Zwecken und anderseits zwischen Übermittlungen an Sicherheitsbehörden anderer Mitgliedstaaten und Übermittlungen an Sicherheitsbehörden von Drittstaaten und an Sicherheitsorganisationen (im Sinne des § 2 Abs. 2 PolKG) zu unterscheiden.

Zu Abs. 1:

Abs. 1 regelt unter welchen Voraussetzungen Übermittlungen zu Zwecken der Sicherheits- und Kriminalpolizei zulässig sind. Z 1 und Z 2 unterscheiden nach dem Übermittlungsempfänger, da nach der DS-RL bzw. dem DSG hierzu unterschiedliche Voraussetzungen bestehen. Z 1 definiert die Voraussetzung für Übermittlungen an Sicherheitsbehörden von Mitgliedstaaten sowie Europol. Gemäß Art 9 Abs. 4 der DS-RL dürfen für Übermittlungen an andere Mitgliedstaaten keine Bedingungen zur Anwendung gelangen, die nicht auf für entsprechende innerstaatliche Datenübermittlungen gelten. Daher sind keine zusätzlichen Auflagen oder Beschränkungen für Datenübermittlungen zulässig, die sich nicht auch innerstaatlich ergeben. Folglich ist eine Übermittlung von österreichischen Sicherheitsbehörden an Sicherheitsbehörden anderer Mitgliedstaaten unter denselben Voraussetzungen zulässig wie nach den nationalen sicherheitspolizeilichen und strafprozessualen Bestimmungen. Das bedeutet, dass dann Auflagen erteilt werden dürfen, wenn diese im Falle einer Übermittlung an eine andere, inländische Behörde aufgrund der nationalen Bestimmungen (beispielsweise im SPG oder in der StPO) ebenfalls vorgesehen sind.

Z 2 regelt unter welchen Voraussetzungen eine Übermittlung personenbezogener Daten zu Zwecken der Sicherheits- und Kriminalpolizei an Sicherheitsbehörden von Drittstaaten sowie Sicherheitsorganisationen gemäß § 2 Abs. 2 Z 2 und 3 zulässig ist. Das DSG gibt konkrete Vorgaben,

welche sich in den Bestimmungen der §§ 58 ff DSG (Art. 35 ff DS-RL) wiederfinden. Nach diesen ist eine Übermittlung personenbezogener Daten zulässig, wenn sie für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs erforderlich ist und an einen für diese Zwecke zuständigen Verantwortlichen erfolgt. Darüber hinaus bedarf es eines Angemessenheitsbeschlusses der Europäischen Kommission bezüglich des konkreten Drittstaates, in Ermangelung eines solchen sonstiger geeigneter Garantien hinsichtlich eines angemessenen Datenschutzniveaus; in bestimmten Ausnahmefällen ist die Übermittlung auch ohne einen Angemessenheitsbeschluss oder geeignete Garantien erlaubt (§ 59 Abs. 6 DSG). Sollen Daten übermittelt werden, die ursprünglich von einem anderen Mitgliedstaat stammen, ist zuvor dessen Zustimmung einzuholen.

Zu Abs. 2:

Abs. 2 regelt die Zulässigkeit der Übermittlung personenbezogener Daten zu Zwecken des Passwesens, der Fremdenpolizei und der Grenzkontrolle. Da diese Zwecke nicht im Anwendungsbereich der DS-RL bzw. des 3. Hauptstücks des DSG liegen, gelangt die DSGVO zur Anwendung. Auch in diesem Fall muss zwischen den Übermittlungsempfängern – Mitgliedstaaten und Drittstaaten sowie Sicherheitsorganisationen – unterschieden werden, da entsprechend unterschiedliche Voraussetzungen zu erfüllen sind. Für Übermittlungen im Anwendungsbereich der DSGVO sollen ebenfalls dieselben Voraussetzungen gelten wie für Übermittlungen innerhalb eines Staates und dürfen daher auch hier keine engeren Voraussetzungen für Übermittlung an Mitgliedstaaten vorgesehen werden, als sie vergleichsweise für eine solche innerstaatliche Übermittlung Anwendung finden. Demnach ist die Übermittlung personenbezogener Daten an Mitgliedstaaten dann zulässig, wenn eine solche zur Erfüllung der Aufgabe erforderlich ist. Dies ist eine Grundvoraussetzung, die auch für Übermittlungen an inländische Behörden vorgesehen ist.

Im Falle der Übermittlung von Daten zu Zwecken des Passwesens, der Fremdenpolizei sowie der Grenzkontrolle an Sicherheitsbehörden von Drittstaaten oder an Sicherheitsorganisationen gemäß § 2 Abs. 2 Z 2 und 3 finden die diesbezüglichen Bestimmungen des Kapitel V der DSGVO Anwendung und verweist Z 2 entsprechend auf diese.

Zu Art. 90 Z 7 bis 13 (§ 8a PolKG):

Es handelt sich um Anpassungen an die datenschutzrechtlichen Vorgaben. Eine materielle Änderung zur bisherigen Rechtslage erfolgt nicht.

Zu Abs. 1:

In dieser Bestimmung wird die Teilnahme an internationalen Datenverarbeitungen den datenschutzrechtlichen Vorgaben angepasst. Das neue Datenschutzregime regelt die Möglichkeit der gemeinsamen Verarbeitung durch zwei oder mehrere Verantwortliche sowohl im rein nationalen Rahmen als auch im grenzüberschreitenden Bereich mit Mitgliedstaaten. Bei den gemeinsamen Datenverarbeitungen iSd § 8a handelt es sich um Datenverarbeitungen sowohl mit Sicherheitsbehörden von Mitgliedstaaten als auch mit Sicherheitsbehörden von Drittstaaten bzw. mit Sicherheitsorganisationen. Eine solche ist zulässig, wenn eine Übermittlung – welches eine Unterform der Verarbeitung darstellt – zulässig ist.

Das bedeutet, dass im Falle einer gemeinsamen Verarbeitung mit Sicherheitsbehörden von Drittstaaten oder mit Sicherheitsorganisationen gemäß § 2 Abs. 2 Z 2 und 3 zu prüfen ist, ob die Voraussetzungen gemäß § 58 ff DSG vorliegen. Dies kann nun sein, dass ein Angemessenheitsbeschluss der Europäischen Kommission oder – in Ermangelung eines solchen – geeignete Garantien zum Schutz personenbezogener Daten gegeben sind. Diese geeigneten Garantien können in einem rechtsverbindlichen Instrument (beispielsweise einem bilateralen Abkommen) festgelegt werden oder der Verantwortliche ist aufgrund der Beurteilung aller relevanten Umstände zu dem Ergebnis gekommen, dass solche geeigneten Garantien zum Schutz personenbezogener Daten vorliegen.

Zu Abs. 2:

Während Abs. 2 Z 1 die Zusammenarbeit mit Interpol konkretisiert, trägt Z 2 dem Umstand Rechnung, dass sich die zivilen Inlands- und Sicherheitsdienste der EU-Staaten sowie Norwegen und Schweiz Ende 2001 auf Initiative einer Sonderinnenministertagung als Reaktion auf die Anschläge vom 11. September 2001 zum Zweck der grenzüberschreitenden Terrorismusbekämpfung zu einer Counter-Terrorism-Group zusammengeschlossen haben, um den Informationsaustausch über eine gemeinsam genutzte Datenbank zu intensivieren. Hierbei handelt es sich um eine Angelegenheit, die nicht dem Recht der Europäischen Union unterliegt (§ 3 Abs. 4 DSG). Die Ausschlüsse der Anwendbarkeit bestimmter Regelungen des DSG auf die Datenverarbeitung nach Z 2 gründet sich insbesondere auf die Nichtanwendbarkeit der

bisherigen § 12 Abs. 5 zweiter Satz und § 50 DSG 2000, welche bislang im letzten Satz des Abs. 1 geregelt war. Diese umfasste sowohl Z 1 als auch Z 2 des Abs. 2. Aufgrund des neuen Datenschutzregimes wird dieser Ausschluss minimiert, indem dieser nur noch für Z 2 zur Anwendung gelangt. Die Zulässigkeit des Ausschlusses für Z 2 zu oben genannten Zwecken ergibt sich aus § 3 Abs. 4 DSG in Zusammenschau mit Art. 2 Abs. 3 lit. a der DS-RL (sowie näher ausgeführt in Erwägungsgrund 14). Um das bisher bestehende hohe Datenschutzniveau auch weiterhin beizubehalten, werden daher lediglich spezifische Bestimmungen des DSG ausgeschlossen, die auch schon bisher nicht zur Anwendung gelangt sind.

Zu Art. 90 Z 14 (§ 9 PolKG):

Im bisherigen Abs. 1 erfolgt eine terminologische Anpassung und wird die Absatzbezeichnung aufgrund der Streichung des Abs. 2 entfernt.

Der bisherige Abs. 2 entfällt, da sich diese Verpflichtung künftig unmittelbar auf § 45 Abs. 6 DSG stützt. Von einer ident lautenden Bestimmung wurde hier Abstand genommen. Nach wie vor sind die Sicherheitsbehörden verpflichtet Daten, die ihnen von ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen übermittelt wurden und die zu löschen sind, ebenfalls zu löschen. Dies ergibt sich nunmehr aus § 45 Abs. 6 DSG. Daten, die in einer gemeinsamen Datenverarbeitung (vormals Informationssammlung) verarbeitet werden, sind nach den jeweiligen völkerrechtlichen Regelungen zu löschen. Die Regelungen hinsichtlich der Speicher- und Löschungsfristen ergeben sich aus den jeweiligen nationalen Materiengesetzen sowie den völkerrechtlichen Regelungen. Eine materielle Änderung zur bisherigen Rechtslage erfolgt nicht.

Zu Art. 90 Z 15 (§ 10 PolKG):

Die Streichung dieser Bestimmung ist der Anwendbarkeit des DSG geschuldet. Die Verpflichtung der Verständigung der ausländischen Sicherheitsbehörde oder der Sicherheitsorganisationen im Falle der Kenntnisnahme unrichtiger, unrechtmäßig verarbeiteter, richtigzustellender oder zu löschender personenbezogener Daten bleibt weiterhin aufrecht. Diese Verpflichtung ergibt sich nunmehr unmittelbar aus § 45 Abs. 5 und 6 DSG. Von einer replizierenden Bestimmung in diesem Gesetz wurde Abstand genommen. Eine materielle Änderung zur bisherigen Rechtslage erfolgt nicht.

Zu Art. 90 Z 16 (§ 11 PolKG):

Es handelt sich um eine Anpassung der Protokollierungsbestimmung an die Vorgaben des § 50 DSG. Die Zuordnung zu einem bestimmten Organwalter ist bei ausschließlich programmgesteuerten (vormalige Diktion: automatisierten) Abfragen nicht erforderlich. Erfasst von dieser Ausnahmebestimmung sind solche Abfragen, die nicht durch eine Willensbetätigung eines Menschen initiiert werden, sondern ausschließlich durch ein Computersystem aufgrund seiner Programmierung vollautomatisch durchgeführt werden. Hierbei ist die Zuordnung zu einem bestimmten Organwalter nicht möglich, da kein Organ, sondern ausschließlich ein Computersystem, tätig wird. Eine ausdrückliche Bestimmung der Aufbewahrungsfrist für Protokolldaten findet sich in § 50 DSG nicht. Aus diesem Grund wird hier eine entsprechende Regelung insofern getroffen, dass Protokolldaten – wie bisher – für mindestens drei Jahre aufzubewahren und anschließend zu löschen sind.

Zu Art. 90 Z 17 (§ 12 PolKG):

Es erfolgt eine konkretisierende Anpassung an das DSG dahingehend, als künftig die in § 43 Abs. 4 DSG taxativ aufgezählten Gründe eine Beschränkung des Auskunftsrechts zulassen. Die Möglichkeit der Beschränkung des Auskunftsrechts ergibt sich aus § 44 Abs. 2 DSG. Im Falle eines Auskunftsbegehrens ist jene ausländische Sicherheitsbehörde oder Sicherheitsorganisation vor Erteilung einer Auskunft um Stellungnahme zu ersuchen, ob eine der Voraussetzungen gemäß § 43 Abs. 4 DSG für eine Beschränkung der Auskunft vorliegt.

Zu Art. 90 Z 19 (§ 20 Abs. 10 PolKG):

Es handelt sich um die erforderlichen Inkrafttretens- und Außerkrafttretensbestimmungen.

Artikel 91 (Änderung des EU-Polizeikooperationsgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“).

Zu Art. 91 Z 1 bis 3 (Inhaltsverzeichnis):

Es handelt sich um notwendige Anpassungen des Inhaltsverzeichnisses

Zu Art. 91 Z 4 und 7 (§§ 1 Abs. 2, 5 Abs. 4 EU-PolKG):

Es handelt sich um eine Zitatanpassung.

Zu Art. 91 Z 5, 7, 9, 10, 11 und 12 (§§ 3 Abs. 1 und 3, 5 Abs. 2, 6 Abs. 1 bis 3, 26, 33 Abs. 1, 3 und 7 EU-PolKG):

Es handelt sich um notwendige terminologische Anpassungen aufgrund der datenschutzrechtlichen Vorgaben. Der Begriff des „Verwendens“ wird durch den umfassenden Begriff des „Verarbeitens“ gemäß § 36 Abs. 2 Z 2 DSG (Art. 3 Z 2 DS-RL) ersetzt. Davon ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten erfasst. Dies umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Eine Differenzierung zwischen den Begriffen „Ermitteln“, „Verwenden“ und „Verarbeiten“ besteht nicht mehr und es werden alle diese gänzlich von „Verarbeiten“ erfasst. Im Sinne der Klarstellung wird jedoch vereinzelt von der Verwendung des umfassenden Begriffs „Verarbeiten“ abgegangen und lediglich von „Ermitteln“ oder „Übermitteln“ gesprochen, um die im jeweiligen Kontext konkret zulässige Form des „Verarbeitens“ klar zu definieren.

Dem bisherigen Begriff des „Auftraggebers“ entspricht nunmehr die Definition des „Verantwortlichen“ (§ 36 Abs. 2 Z 8 DSG, Art. 3 Z 8 DS-RL) und wird damit die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, definiert.

Dem Begriff der „Datenanwendung“ (§ 4 Z 7 DSG 2000) entspricht nunmehr der Terminus der „Datenverarbeitung“.

Zu Art. 91 Z 6 (§ 4 Abs. 1 EU-PolKG):

Es handelt sich um die Bereinigung eines Redaktionsversehens.

Zu Art. 91 Z 8 (Überschriften zu §§ 6, 22 und 24 EU-PolKG):

Die vorgeschlagenen Änderungen der Überschriften dienen der terminologischen Anpassung an das DSG.

Zu Art. 91 Z 13 (§ 43 EU-PolKG):

Es handelt sich um eine Konkretisierung der bestehenden Regelung. Im Falle eines Auskunftsbegehrens ist vor Erteilung einer Auskunft – wie bisher – jener Mitgliedstaat, der die Daten eingeben hat, um Stellungnahme zu ersuchen, ob einer der in § 43 Abs. 4 DSG genannten Gründe für eine Beschränkung der Auskunft vorliegt.

Im Übrigen erfolgt eine Zitatanpassung.

Zu Art. 91 Z 14 (§ 46 Abs. 7 EU-PolKG):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Art. 92 (Änderung des Bundespräsidentenwahlgesetzes 1971)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 92 Z 1 (§ 25a BPräsWG):

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 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 § 25a für sämtliche nach dem Bundespräsidentenwahlgesetz 1971 verarbeitete Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Wahlrechts ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes

schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Wahlen steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug von an ein striktes Fristengefüge gebundenen Wahlereignissen nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, so sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 92 Z 2 (§ 28 Abs. 14 BPräsWG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 93 (Änderung des Europäische-Bürgerinitiative-Gesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 2 B-VG („Wahlen zum Europäischen Parlament; Europäische Bürgerinitiativen“).

Zu Art. 93 Z 1, Z 2 und Z 3 (§ 3 Abs. 2, § 3 Abs. 6 und § 3 Abs. 8 EBIG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die DSGVO (Art. 4 DSGVO). Demnach sollen die Begriffe „Datei“ und „Datenbank“ durch „Dateisystem“ ersetzt werden.

Zu Art. 93 Z 4 (§ 3 Abs. 9 EBIG):

Eine Datenverarbeitung muss gemäß Art. 9 Abs. 2 lit. g DSGVO der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen. Das Europäische-Bürgerinitiative-Gesetz dient, wie § 1 Abs. 1 ausführt, der Durchführung der Verordnung (EU) Nr. 211/2011 über die Bürgerinitiative, ABl. Nr. L 65 vom 11.03.2011 S. 1. Der Zweck der Verarbeitung von Daten im Sinne des Europäische-Bürgerinitiative-Gesetzes liegt somit in der Erfüllung einer unionsrechtlichen Verpflichtung.

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 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 § 3 Abs. 9 für sämtliche nach dem Europäische-Bürgerinitiative-Gesetz verarbeitete Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Europäische-Bürgerinitiative-Gesetzes ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Europäischen Bürgerinitiativen, die in Art. 11 Abs. 4 des EU-Vertrages verankert sind, steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der der Behörde übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt, ein geordneter, sparsamer und effizienter an ein striktes Fristengefüge gebundener Vollzug nicht mehr möglich und es könnte den unionsrechtlichen Verpflichtungen bezüglich der Europäischen Bürgerinitiative nicht nachgekommen werden. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

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 öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information

kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 93 Z 5 (§ 10 Abs. 4 EBIG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 94 (Änderung des Europa-Wählerevidenzgesetzes)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 2 B-VG („Wahlen zum Europäischen Parlament; Europäische Bürgerinitiativen“).

Zu Art. 94 Z 1 (§ 13 Abs. 4 EuWEG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). Demnach soll der Begriff „verwenden“ durch „verarbeiten“ ersetzt werden.

Zu Art. 94 Z 2 (§ 13 Abs. 5 EuWEG):

Eine Datenverarbeitung muss gemäß Art. 9 Abs. 2 lit. g DSGVO der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen. Die Führung einer ständigen Europa-Wählerevidenz ist, wie § 1 Abs. 1 ausführt, die Grundlage für das Anlegen von Wählerverzeichnissen vor einer Wahl zum Europäischen Parlament. Der Zweck der Verarbeitung von Daten im Sinne des Europa-Wählerevidenzgesetzes liegt somit in der Erfüllung einer unionsrechtlichen Verpflichtung.

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 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 § 13 Abs. 5 für sämtliche nach dem Europa-Wählerevidenzgesetz verarbeitete Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Europa-Wählerevidenzgesetzes ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Europawahlen steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der der Behörde übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen. Es wäre nicht mehr gewährleistet, dass in der Europa-Wählerevidenz oder in den daraus

generierten Wählerverzeichnissen alle Wahlberechtigten enthalten sind und ein an ein striktes Fristengefüge gebundener Vollzug von Europawahlen wäre nicht mehr möglich, sodass den unionsrechtlichen Verpflichtungen bezüglich der Wahl zum Europäischen Parlament nicht nachgekommen werden könnte.

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 öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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 Funktionalität und Zweck der Führung der Europa-Wählerevidenz gewährleisten. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 94 Z 3 (§ 20 Abs. 12 EuWEG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 95 (Änderung der Europawahlordnung)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 2 B-VG („Wahlen zum Europäischen Parlament; Europäische Bürgerinitiativen“).

Zu Art. 95 Z 1 (§ 11 Abs. 1 EuWO):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). Demnach soll der Begriff „EDV-Applikation“ durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 95 Z 2 (§ 11 Abs. 5 EuWO):

Eine Datenverarbeitung muss gemäß Art. 9 Abs. 2 lit. g DSGVO der Verwirklichung eines wichtigen, im Unions- oder nationalen Recht anerkannten Interesses dienen. Die österreichischen Mitglieder des Europäischen Parlaments im Sinne des Art. 23a B-VG werden, wie § 1 Abs. 1 ausführt, nach den Bestimmungen der Europawahlordnung gewählt. Der Zweck der Verarbeitung von Daten im Sinne dieses Bundesgesetzes liegt somit in der Erfüllung einer unionsrechtlichen Verpflichtung.

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 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 § 11 Abs. 5 für sämtliche nach der Europawahlordnung verarbeitete Daten Gebrauch gemacht.

Für einen geordneten Vollzug der Europawahlordnung ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Europawahlen steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der der Behörde übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen. Eine an ein striktes Fristengefüge gebundene Durchführung von Europawahlen wäre nicht mehr möglich, sodass den unionsrechtlichen Verpflichtungen bezüglich der Wahl zum Europäischen Parlament nicht nachgekommen werden könnte.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, so sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 95 Z 3, Z 4 und Z 5 (§ 34 Abs. 1, § 39 Abs. 8 und § 72 Abs. 6 EuWO):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So sollen die Begriffe „zur Verfügung stellen“ durch „übermitteln“ und „Datei“ durch „Dateisystem“ ersetzt werden.

Zu Art. 95 Z 6 (§ 91 Abs. 15 EuWO):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 96 (Änderung der Nationalrats-Wahlordnung 1992)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 96 Z 1, Z 3, Z 4 und Z 5 (§ 23 Abs. 1, § 46 Abs. 1, § 52 Abs. 7 und § 106 Abs. 5 NRWO):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So sollen die Begriffe „EDV-Applikation“ durch „Datenverarbeitung“, „zur Verfügung stellen“ durch „übermitteln“ und „Datei“ durch „Dateisystem“ ersetzt werden.

Zu Art. 96 Z 2 (§ 23 Abs. 5 NRWO):

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 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 § 23 Abs. 5 für sämtliche nach der Nationalrats-Wahlordnung 1992 verarbeitete Daten Gebrauch gemacht.

Für einen geordneten Vollzug des Wahlrechts ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Wahlen steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug von an ein striktes Fristengefüge gebundenen Wahlereignissen nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, so sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen

Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 96 Z 6 (§ 129 Abs. 12 NRWO):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 97 (Änderung des Volksabstimmungsgesetzes 1972)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 97 Z 1 (§ 6 Abs. 3 VAbstG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So soll der Begriff „EDV-Applikation“ durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 97 Z 2 (§ 19 Abs. 3 VAbstG):

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 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 § 19 Abs. 3 für sämtliche nach dem Volksabstimmungsgesetz 1972 verarbeitete Daten Gebrauch gemacht.

Für eine geordnete Durchführung von Volksabstimmungen ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Volksabstimmungen steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des strikten Fristengefüges bei Volksabstimmungen nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, so sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 97 Z 3 (§ 21 Abs. 9 VAbstG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 98 (Änderung des Volksbefragungsgesetzes 1989)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 98 Z 1 (§ 6 Abs. 3 VBefrG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So soll der Begriff „EDV-Applikation“ durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 98 Z 2 (§ 20 Abs. 4 VBefrG):

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 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 § 20 Abs. 4 für sämtliche nach dem Volksbefragungsgesetz 1989 verarbeitete Daten Gebrauch gemacht.

Für eine geordnete Durchführung von Volksbefragungen ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Volksbefragungen steht im allgemeinen öffentlichen Interesse; die

gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des strikten Fristengefüges bei Volksbefragungen nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

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 öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 98 Z 3 (§ 21 Abs. 10 VBefrG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 99 (Änderung des Volksbegehrengesetzes 2018)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 99 Z 1 (§ 4 Abs. 4 VoBeG):

Die vorgeschlagene Bestimmung, wonach Registrierungen von Volksbegehren und Vermerke über getätigte Unterstützungserklärungen zu löschen sind, wenn ein Einleitungsantrag abgewiesen wurde und die Abweisung eines Volksbegehrens unanfechtbar feststeht, dient den in der DSGVO normierten Grundsätzen der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

Zu Art. 99 Z 2, Z 4, Z 8, Z 9, Z 12 und Z 14 (§ 5 Abs. 1 Z 1, § 5 Abs. 2, § 6 Abs. 1, § 11 Abs. 1 Z 1, § 11 Abs. 2 und § 13 Abs. 1 VoBeG):

Die vorgeschlagenen Änderungen dienen der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So soll der Begriff „Datenanwendung“ jeweils durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 99 Z 3 und Z 11 (§ 5 Abs. 2 und § 11 Abs. 2 VoBeG):

Es wird eine grammatikalische Klarstellung von durch ein Redaktionsversehen unvollständig gebliebenen Satzteilen vorgenommen.

Zu Art. 99 Z 5 (§ 5 Abs. 2 VoBeG):

Mit der vorgeschlagenen Bestimmung wird eine Klarstellung vorgenommen, was mit einem unterschriebenen Unterstützungserklärungs-Formular zu geschehen hat, wenn ein Einleitungsantrag abgewiesen wurde und eine Anfechtung nicht mehr möglich ist oder ein Einleitungsantrag bis zum Ablauf des 31. Dezember des dem Jahr, in dem die Anmeldung vorgenommen wurde, folgenden Jahr nicht gestellt wurde. Die unverzügliche Vernichtung des Formulars durch die Gemeinde nach entsprechender Verständigung durch den Bundesminister für Inneres dient den in der DSGVO normierten Grundsätzen der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

Zu Art. 99 Z 6 und Z 7 (§ 5 Abs. 3 und § 5 Abs. 4 VoBeG):

Es wird eine terminologische Angleichung an die übrigen Formulierungen in § 5 vorgeschlagen, da in der Phase der Abgabe von Unterstützungserklärungen generell von „Unterstützungswilligen“ gesprochen wird; in diesem Sinne soll auch eine terminologische Angleichung des Wortes „Eintragung“ hin zur Wendung „Abgabe einer Unterstützungserklärung“ erfolgen. Mit dem Entfall des Verweises auf „Vorschriften des Abschnittes III“ wird ein Redaktionsversehen behoben.

Zu Art. 99 Z 9 (§ 6 Abs. 5 VoBeG):

Es wird eine notwendige terminologische Angleichung vorgenommen, da in der Eintragungsphase generell von „Eintragung“ gesprochen wird.

Zu Art. 99 Z 11 (§ 11 Abs. 2 VoBeG):

Es wird eine Klarstellung der Verweisung vorgeschlagen, da im Eintragungsverfahren hinsichtlich der Stimmberechtigung auf die *lex specialis* des § 7 des Volksbegehrengesetzes 2018 abgestellt wird.

Zu Art. 99 Z 14 (§ 11 Abs. 5 VoBeG):

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 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 § 11 Abs. 5 für sämtliche nach dem Volksbegehrengesetz 2018 verarbeitete Daten Gebrauch gemacht.

Für eine geordnete Durchführung von Volksbegehren ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Volksbegehren steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug des strikten Fristengefüges bei Volksbegehren nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen.

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 öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 99 Z 16 (§ 24 VoBeG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zu Art. 100 (Änderung des Wählerevidenzgesetzes 2018)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich dieses Artikels auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung, insbesondere Wahlen zum Nationalrat, und Volksbegehren, Volksabstimmungen und Volksbefragungen auf Grund der Bundesverfassung“).

Zu Art. 100 Z 1 (§ 2 Abs. 7 WEviG):

Die vorgeschlagene Änderung dient der terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO). So soll der Begriff „verwenden“ durch „verarbeiten“ ersetzt werden.

Zu Art. 100 Z 2 (§ 4 Abs. 1 WEviG):

Der DSGVO und – soweit es diese in seinem 1., 2. und 4. Hauptstück umsetzt – dem Datenschutzgesetz (DSG), BGBl. I Nr. 120/2017, ist der Begriff des Informationsverbundsystems (bisher § 4 Z 13 DSG 2000) unbekannt. Die vorgeschlagene Änderung dient der terminologischen Anpassung an die DSGVO. Art. 26 DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll § 4 Abs. 1 entsprechend angepasst werden. Eine materielle Änderung gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der Zentralen Evidenz verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – z. B. Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene § 4 Abs. 1 die Zuständigkeit zwischen den gemeinsam Verantwortlichen der zentralen Evidenz dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll nach Abs. 1 direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen.

Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den gemäß dem ersten Satz zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Gemäß Art 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Diese Funktionen übte in Bezug auf das Zentrale Wählerregister bisher der Bundesminister für Inneres aus, weshalb es im Sinne größtmöglicher Kontinuität angezeigt ist, ihm künftig durch Abs. 1 die Funktion des Auftragsverarbeiters zu übertragen. Zudem soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen sowie datenqualitätssichernde Maßnahmen zu setzen, wie insbesondere Hinweise auf eine mögliche Identität zweier ähnlicher Datensätze oder die Schreibweise von Adressen zu geben („Clearing“). Darüber hinaus darf er – wie bisher – weitere Auftragsverarbeiter in Anspruch nehmen.

Zu Art. 100 Z 3 (§ 4 Abs. 3 WEviG):

§ 14 DSG 2000 sieht 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. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. 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, in § 4 Abs. 3 eine dem § 14 Abs. 2 Z 7 DSG 2000 vergleichbare Regelung aufzunehmen, wobei die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden soll.

Weiters soll in § 4 Abs. 3 im Sinne einer terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO) der Begriff „Datenanwendung“ durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 100 Z 4 (§ 4 Abs. 4 WEviG):

Im Sinne einer terminologischen Anpassung an die Definitionen der DSGVO (Art. 4 DSGVO) soll der Begriff „Datenanwendung“ durch „Datenverarbeitung“ ersetzt werden.

Zu Art. 100 Z 5 (§ 4 Abs. 6 WEviG):

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 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 § 4 Abs. 6 für sämtliche nach dem Wählerevidenzgesetz 2018 verarbeitete Daten Gebrauch gemacht.

Für eine geordnete Durchführung von Wahlereignissen ist die Verarbeitung personenbezogener Daten in Wählerevidenzen in dem gesetzlich vorgesehenen Maße unerlässlich und es liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Die rechtskonforme, fristgerechte Durchführung von Wahlen bzw. Volksbegehren steht im allgemeinen öffentlichen Interesse; die gesetzlich vorgesehene Verarbeitung der betreffenden Daten ist daher zur Erfüllung der den Behörden übertragenen Aufgaben – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz von vorherein wesentlich beeinträchtigt und ein geordneter, sparsamer und effizienter Vollzug nicht mehr möglich. Die Ausübung der Rechte gemäß Art. 18 und 21 DSGVO – die auch nach bisheriger Rechtslage nicht vorgesehen sind – würde zudem einen beträchtlichen Verwaltungsaufwand verursachen. Es wäre nicht mehr gewährleistet, dass in der Wählerevidenz oder in den daraus generierten Wählerverzeichnissen alle Wahlberechtigten enthalten sind und ein geordneter, an ein striktes Fristengefüge gebundener Vollzug von Wahlereignissen wäre nicht mehr möglich.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, so sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an öffentlich-rechtliche 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 Betroffenen bleibt es auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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 und 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 ist im letzten Satz allerdings vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind, wobei diese Information nicht an jeden einzelnen Betroffenen individuell zu richten ist, sondern an „die Betroffenen“ in deren Gesamtheit. Die Information kann daher auch in allgemeiner Weise erteilt werden (zum Beispiel auf der Homepage des Bundesministeriums für Inneres).

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 Funktionalität und Zweck der Führung des zentralen Wählerregisters gewährleisten. Aus diesen Gründen wird vorgeschlagen, das Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung auszuschließen.

Zu Art. 100 Z 6 (§ 19 WEviG):

Diese Bestimmung regelt das Inkrafttreten der Änderung dieses Bundesgesetzes.

Zum 8. Hauptstück (Justiz)

Allgemeines

1. Die Datenschutz-Grundverordnung (kurz: DSGVO) tritt am 25. Mai 2018 in Geltung.

Die Datenschutz-Grundverordnung gilt gemäß ihrem Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Sie nimmt die Tätigkeit der Justiz nicht generell von ihrem sachlichen Anwendungsbereich aus; von diesem ausgenommen sind lediglich Datenverarbeitungen in den in Art. 2 Abs. 2 DSGVO genannten Bereichen. Gemäß Art. 2 Abs. 2 lit. d gilt die DSGVO nicht für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Die DSGVO gilt daher grundsätzlich für jegliches im Zusammenhang mit einem zivilgerichtlichen Verfahren oder der Tätigkeit in Angelegenheiten der Justizverwaltung ermitteltes personenbezogenes Datum, welches elektronisch (in der Verfahrensautomation Justiz oder in Hinkunft im System der Justiz 3.0) gespeichert wird.

Die DSGVO sieht für den Bereich der justiziellen Tätigkeit lediglich partielle Ausnahmen ihrer Geltung vor. Gemäß Art. 37 Abs. 1 lit. a DSGVO muss kein Datenschutzbeauftragter benannt werden, wenn die Datenverarbeitung von Gerichten vorgenommen wird, die im Rahmen ihrer justiziellen Tätigkeit handeln. Weiters sind gemäß Art. 55 Abs. 3 DSGVO die Aufsichtsbehörden (in Österreich: die Datenschutzbehörde) für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig.

Die DSGVO enthält, wie bereits an weiter oben erwähnt, sogenannte „Öffnungsklauseln“, also fakultative Regelungsspielräume, die den Mitgliedstaaten im sachlichen Anwendungsbereich der Verordnung abweichende oder in bestimmten Bereichen den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten.

In diesem Sinn eröffnet Art. 23 DSGVO die Möglichkeit, durch Rechtsvorschriften der Union oder der Mitgliedstaaten die Pflichten und Rechte gemäß den Art. 12 bis 22 und 34 DSGVO gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Solche Beschränkungen sind überdies nur zur Sicherstellung bestimmter, in den in Art. 23 Abs. 1 lit. a bis j DSGVO angeführter Schutzzwecke zulässig, so etwa zum Schutz der Unabhängigkeit der Justiz und zum Schutz von Gerichtsverfahren (lit. f), zur Sicherstellung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe (lit. g), zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen (lit. i) und zur Sicherstellung der Durchsetzung zivilrechtlicher Ansprüche (lit. j).

Die in den Art. 12 bis 22 und 34 DSGVO angeführten Datenschutzrechte des Einzelnen, die in obigem Sinn gesetzlich eingeschränkt werden können, betreffen etwa das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung.

Die Umsetzung des durch die Öffnungsklauseln eingeräumten gesetzgeberischen Gestaltungsspielraums soll in den spezifischen Materiengesetzen erfolgen.

2. Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Tätigkeit der ordentlichen Gerichtsbarkeit erfordern es, dass von der genannten Öffnungsklausel des Art. 23 DSGVO Gebrauch gemacht wird, um die Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren gewährleisten zu können. Der vorliegende Entwurf sieht daher spezifische Bestimmungen für den Bereich der Justiz und die in enger Verbindung mit der Justiz stehenden Berufsgruppen der Rechtsanwälte und Notare vor.

2.1. Für das zivilgerichtliche Verfahren wird einerseits der Begriff der justiziellen Tätigkeit näher definiert und für das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung, soweit es sich auf den Bereich dieser justiziellen Tätigkeit bezieht, auf die Verfahrensrechte verwiesen. Andererseits wird für die Verletzung des Grundrechts auf Datenschutz ein eigener Feststellungsanspruch, wie er bereits derzeit bei Datenschutzverletzungen durch ein Organ der Gerichtsbarkeit besteht, vorgesehen.

2.2. Darüber hinaus sieht der Entwurf punktuelle Anpassungen im Zivilverfahrensrecht vor, die in der gerichtlichen Praxis derzeit strittige datenschutzrechtliche Fragen auf eine klare gesetzliche Basis stellen sollen.

- Einführung eines Rechtsschutzmechanismus für den Fall, dass ein (inländisches) Gericht einem anderen (inländischen) Gericht die Rechtshilfe durch Übersendung des Gerichtsakts versagt.
- Klärung der Frage, unter welchen Voraussetzungen von Gerichten auf Ersuchen inländischer Verwaltungsbehörden Amtshilfe durch Übersendung von Akten oder Aktenbestandteilen geleistet werden muss.
- Vorgaben für die Veröffentlichung eines Verhandlungsspiegels durch die Gerichte.
- Regelung des Auskunftsrechts von Bürgern über Abfragen des Personenverzeichnisses im Grundbuch durch Notare und Rechtsanwälte.
- Anpassung begrifflicher Änderungen durch die DSGVO.

3. Da der Anwendungsbereich der DSGVO auch das anwaltliche und notarielle Berufsrecht betrifft, werden mit dem Entwurf entsprechende Regelungen in der RAO, in der NO und im DSt vorgeschlagen, die den besonderen Verfahrenszwecken der durch die Rechtsanwälte und Notare geführten Archive, Verzeichnisse und Register (insbesondere Urkundenarchiv, Treuhandregister, ÖZVV und ÖZTR), dem Schutz der berufsrechtlichen Verschwiegenheitspflichten und der Sicherstellung des geordneten Ablaufs von Disziplinarverfahren Rechnung tragen sollen. Die hier vorgesehenen Beschränkungen des Datenschutzrechts und der Begleitrechte nach der DSGVO beziehen sich im Wesentlichen auf die Tatbestände des Art. 23 Abs. 1 lit. g, i und j DSGVO. Auch in diesen Bereichen sollen die besonderen Archiv-, Register- und Verfahrenszwecke dadurch gewahrt werden, dass anstelle der sich aus den Art. 12 bis 22 und 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten die jeweils spezifischen Verfahrensregelungen von RAO, NO, DSt sowie GOG und der damit im Zusammenhang im selbständigen Wirkungsbereich erlassenen berufsständischen Richtlinien zur Anwendung kommen.

4. Die für den Bereich des Strafrechts geltende Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: DS-RL), ABl. Nr. L 119 vom 4.5.2016 S. 89, wurde durch das Datenschutz-Anpassungsgesetz 2018 und die darin vorgesehenen Anpassungen im Datenschutzgesetz (DSG) idF BGBl. I Nr. 120/2017 umgesetzt.

In dessen 3. Hauptstück finden sich explizite Regelungen zur Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung (§§ 36 ff). Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausdrücklich klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor.

Die bestehenden datenschutzrechtlichen Regelungen der StPO sind daher in erster Linie an die Terminologie der DS-RL (bzw. des DSG) anzugleichen. Ferner soll eine Kriminalpolizei, Staatsanwaltschaft und Gericht gleichermaßen umfassende gesetzliche Grundlage für die grundsätzliche Zulässigkeit der Datenverarbeitung direkt in der StPO verankert und die Akteneinsicht zu wissenschaftlichen Zwecken an die europarechtlichen Vorgaben angepasst werden. Des Weiteren soll der bestehende (subsidiäre) Rechtsschutz des GOG auch weiterhin sowohl im gerichtlichen als auch staatsanwaltschaftlichen Bereich bestehen bleiben.

5. Das der Evidenthaltung strafgerichtlicher Verurteilungen dienende Strafregister unterliegt den unmittelbar anwendbaren Vorschriften der DSGVO. Das StRegG ist daher in erster Linie terminologisch an die Vorgaben der DSGVO anzupassen. Um die dem StRegG (im Einklang mit dem TilgG) wesensimmanenten Schutzzwecke nicht zu unterlaufen, soll ferner klargestellt werden, dass Auskünfte nach der DSGVO ausschließlich in Form einer Strafregisterbescheinigung ergehen sollen.

6. Die DS-RL enthält allerdings auch Regelungen, die den Zuständigkeitsbereich des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz berühren (s. Kapitel V [„Datenübermittlung an Drittländer oder internationale Organisationen“] und Kapitel VI [„Unabhängige Aufsichtsbehörden“]) und einer Umsetzung bedürfen.

II. Besonderer Teil

Zu Art. 101 (Änderung des Auslieferungs- und Rechtshilfegesetzes):

Zu Z 1 (§ 9a ARHG):

Abs. 1 dieser Bestimmung legt in Umsetzung von Art. 35 bis 38 RL-DS, die Voraussetzungen für die in Erledigung eines Rechtshilfeersuchens erfolgende Übermittlung personenbezogener Daten an einen Drittstaat oder eine internationale Organisation fest, wobei diese kumulativ vorzuliegen haben. Im Hinblick auf den Inhalt von § 50 ARHG ist regelmäßig vom Vorliegen der Voraussetzungen nach Z 1 auszugehen.

Für den Fall, dass die übermittelten Daten aus einem anderen Mitgliedstaat stammen, setzt die Datenübermittlung grundsätzlich das Vorliegen der Zustimmung der zuständigen Behörde des betreffenden Mitgliedstaats voraus (s. Abs. 1 Z 2). Die zulässigen Ausnahmen sind in Abs. 2 angeführt. In einem solchen Fall ist die zuständige Behörde unverzüglich von der Datenweiterleitung in Kenntnis zu setzen.

Es ist davon auszugehen, dass die in Abs. 1 Z 3, erster Fall angeführten Voraussetzungen in den seltensten Fällen vorliegen werden, zumal Kommissionsentscheidungen betreffend das Vorliegen eines angemessenen Datenschutzniveaus bisher nur in Bezug auf die Schweiz, Argentinien, Guernsey, die Insel Man, Jersey, die Färöer Inseln, Andorra, Uruguay und Neuseeland ergangen sind.

Abs. 1 Z 3, zweiter Fall betrifft entsprechend Art. 37 Abs. 1 RL DS das Vorliegen angemessener Garantien für den Schutz personenbezogener Daten im betreffenden Staat oder der internationalen Organisation, wobei diese entweder in einem anwendbaren Rechtsinstrument enthalten sein können oder im Einzelfall über entsprechende Nachfrage zugesichert werden (s. lit. a und b *leg. cit*.).

Festzuhalten ist, dass die Angemessenheit der Garantien im Einzelfall entsprechend Art. 37 Abs. 1 lit. b RL DS nach Prüfung aller Umstände, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, vom „Verantwortlichen“ zu beurteilen ist, wobei es sich bei diesem um die aktenführende Behörde (Staatsanwaltschaft oder Gericht) handelt. Durch die angemessenen Garantien soll sichergestellt werden, dass die Datenschutzvorschriften und die Rechte des Betroffenen, einschließlich seines Rechts auf wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe, beachtet werden. Zu berücksichtigen wäre dabei u.a., dass die Übermittlung personenbezogener Daten dem Grundsatz der Spezialität unterliegt, damit gewährleistet ist, dass die Daten nicht zu anderen Zwecken als zu jenen, zu denen sie übermittelt wurden, verarbeitet werden. Darüber hinaus sollte berücksichtigt werden, dass die personenbezogenen Daten nicht verwendet werden, um die Todesstrafe oder eine grausame und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken. Diese Bedingungen können grundsätzlich als geeignete Garantien angesehen werden, doch können vom Verantwortlichen darüber hinaus zusätzliche Garantien verlangt werden.

Ungeachtet des Nichtvorliegens der Voraussetzungen nach Abs. 1 Z 3 ist die in Erledigung eines Rechtshilfeersuchens erfolgende Datenübermittlung in den in Abs. 4 genannten Fällen zulässig, wobei wohl regelmäßig von Vorliegen der Voraussetzungen nach Z 4 auszugehen ist. Festzuhalten ist, dass die Entscheidung im jeweiligen Einzelfall zu treffen ist, wobei zu prüfen ist, ob die Grundrechte des Betroffenen das öffentliche Interesse an der Datenübermittlung überwiegen.

Bei der in Abs. 3 genannten Aufsichtsbehörde handelt es sich gegenständlich um die Oberstaatsanwaltschaft. Der Datenschutzbehörde kommt diesbezüglich keine Zuständigkeit zu: Die Bestimmungen über deren Aufgaben nach § 32 DSG sind in den Fällen der Z 4, 5 und 8 im Bereich der StPO nicht anwendbar, weil in Fällen behaupteter Datenschutzverletzungen in diesen Bereichen ohnehin ein umfassender gerichtlicher Rechtsschutz besteht (s. § 34a Abs. 2a StAG idF BGBl I Nr. XX/2018 samt Erläuterungen), sodass für ein kontrollierendes Eingreifen der Datenschutzbehörde kein Bedarf besteht.

Abs. 5 statuiert entsprechend Art. 38 Abs. 3 RL DS Dokumentationspflichten für den Fall der Datenübermittlung nach Abs. 4. Diese treffen wiederum den Verantwortlichen, somit die aktenführende Behörde. Im Fall der Weiterleitung personenbezogener Daten auf diplomatischem Weg ist die betreffende Verpflichtung für seinen Bereich vom BMEIÄ wahrzunehmen.

Vor dem Hintergrund der elektronischen Aktenführung („ELAK“) und der VJ ist davon auszugehen, dass dadurch den Dokumentationspflichten im Justizbereich ausreichend Rechnung getragen wird.

Zu Z 2 (§ 58a):

Diese Bestimmung enthält in Umsetzung von Art. 35 Abs. 1 lit. e RL DS eine demonstrative Anführung jener Umstände, die von der gemäß § 55 zuständigen österreichischen Behörde, die entsprechend § 9a Abs. 1 Z 2 um Zustimmung zur Weiterleitung personenbezogener Daten, die in Erledigung eines

Rechtshilfeersuchens an einen Drittstaat übermittelt wurden, an einen weiteren Drittstaat oder eine weitere internationale Organisation ersucht wurde, zu berücksichtigen sind.

Zu Z 3 (§ 59a):

Die Datenschutzbestimmung des § 9a idF Z 1 ARHG des Entwurfs gilt vorbehaltlich der Übergangsbestimmung (s. Z 5) für jede Übermittlung personenbezogener Daten durch eine zuständige Behörde, somit auch für die in § 59a ARHG vorgesehene Datenübermittlung ohne Ersuchen. Die in **Abs. 2** dieser Bestimmung enthaltenen Datenschutzbestimmungen hätten daher zu entfallen.

Zu Z 4 (§ 71a):

Art. 39 RL DS sieht unter bestimmten Voraussetzungen die unmittelbare Übermittlung personenbezogener Daten an Empfänger in Drittstaaten vor. Zwar umfasst der Begriff „Empfänger" nach der RL DS neben natürlichen oder juristischen Personen auch „Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden", doch soll diese Bestimmung, bei der es sich um eine Kann-Regelung handelt, nur in Bezug auf Personen umgesetzt werden, um eine gesetzliche Grundlage für die unmittelbare Befassung von in Drittstaaten niedergelassenen Providern zu schaffen. Diesbezüglich sind in der Praxis Probleme aufgetreten, da derartige Ersuchen etwa von den zuständigen amerikanischen Behörden keiner Erledigung zugeführt werden; vielmehr wird die ersuchende Behörde aufgefordert, sich unmittelbar mit dem Provider in Verbindung zu setzen, weshalb davon auszugehen ist, dass dieser zur Erteilung entsprechender Informationen an ausländische Behörden ohne weiteres behördliches Dazwischentreten berechtigt ist. Im Hinblick darauf, dass die Befassung des ausländischen Providers wohl regelmäßig durch die entsprechend zu beauftragenden Sicherheitsbehörden erfolgen wird, soll im Einklang mit der österreichischen Rechtslage klargestellt werden, dass eine derartige Vorgangsweise nur in Bezug auf Ersuchen um Übermittlung von Stammdaten, nicht jedoch auch von Verkehrsdaten und Zugangsdaten in Betracht kommt, weil bei Letzteren in der StPO eine qualifizierte Anordnung vorgesehen und sonst eine gerichtliche Bewilligung erforderlich ist (s. § 76a Abs. 2 StPO, § 5 Abs. 5 StAG).

Zu Z 5 (§ 77 Abs. 4):

Diese Bestimmung regelt das Inkrafttreten der §§ 9a, 58a, 59a und 71a und des Art. XXV. Es wird ein Inkrafttreten mit 25. Mai 2018 vorgesehen.

Zu Z 6 (Übergangsbestimmung):

Diese Bestimmung stellt in Umsetzung von Art. 61 der Datenschutz-RL klar, dass die Datenschutzbestimmung des § 9a auf vor dem 6.5.16 abgeschlossene und mit dem vor diesem Zeitpunkt bestehenden Unionsrecht vereinbare bi- und multilaterale Verträge, die zur Übermittlung personenbezogener Daten führen, keine Anwendung findet. Dies ist eine Folge des Grundsatzes, wonach durch (hier: EU-) Rechtsinstrumente nicht in bestehende Verträge mit Dritten eingegriffen werden kann. Zu denken wäre hier insbesondere an die bestehenden Übereinkommen des Europarats über die justizielle Zusammenarbeit in Strafsachen.

Zu Art. 102 (Änderung des Bewährungshilfegesetzes):

Zu Z 1 (§§ 3 Abs. 1, 4 Abs. 1 und 3, 5 Abs. 3, 8 Abs. 1, 9, 10, 11, 12 Abs. 1, 13 Abs. 1, 2, 4, 6 und 7, 14, 24 Abs. 1, 3 und 4, 26 Abs. 1 Z 3, 26a Abs. 1, 2 und 3, 28 Abs. 1, 2 und 3, 29 Abs. 1, 29d Abs. 1 lit. b und 31 BewHG):

Mit den vorgeschlagenen Änderungen soll die Erweiterung des Bundesministeriums für Justiz zum Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz durch die Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, nachvollzogen werden.

Zu Z 2 (§ 25 BewHG):

Die vorgeschlagenen Änderungen dienen der Anpassung an die DSGVO sowie das DSG („Verarbeitung" statt „Verwendung", „personenbezogene Daten" statt „sensible Daten" sowie – wenngleich nicht unmittelbar anwendbar – der Einführung von § 38 DSG idF BGBl. I Nr. 120/2017 entsprechenden Kautelen).

Die Verarbeitung von Daten nach Art. 9 DSGVO ist regelmäßig eine notwendige Voraussetzung zur Erfüllung der im Bewährungshilfegesetz geregelten sozialarbeiterischen Aufgaben. So ist beispielsweise die Betreuung eines nach § 278b StGB verurteilten Klienten in der Bewährungshilfe oft nicht sinnvoll möglich, ohne Daten zu seinen religiösen oder weltanschaulichen Überzeugungen zu verarbeiten und die Betreuung eines nach § 206 StGB verurteilten Klienten erfordert die Verarbeitung von Daten zu seinem Sexualleben oder zu seiner sexuellen Orientierung. Die Durchführung eines Tatausgleichs wegen § 83 StGB kann die Verarbeitung von Gesundheitsdaten erfordern, genauso, wie die Vermittlung

gemeinnütziger Leistungen im Fall von vermittlungsrelevanten gesundheitlichen Vorbelastungen. Auch bei der Erhebung und Betreuung während des Strafvollzugs durch elektronisch überwachten Hausarrest, in der Entlassenenhilfe und bei der Durchführung von Sozialnetzkonferenzen besteht regelmäßig die Notwendigkeit zur Verarbeitung besonderer Kategorien personenbezogener Daten.

Für die Löschung der personenbezogenen Daten gilt Art. 17 Abs. 1 DSGVO, d.h., dass sie zu dem Zeitpunkt zu löschen sind, zu dem sie nicht mehr (etwa nach Ablauf der Zeit, für die Bewährungshilfe angeordnet wurde) benötigt werden. Für NEUSTART als privater Verein gilt das DSG außer dem 3. Hauptstück und die DSGVO. Das DSG selbst verweist in § 4 ganz allgemein auf die DSGVO, sodass sich die Löschungsverpflichtungen aus dieser unmittelbar anzuwendenden Verordnung ergeben.

Zu Art. 103 (Änderung des Disziplinarstatuts für Rechtsanwälte und Rechtsanwaltsanwärter):

Zu Z 1 (§ 20 DSt):

Zum vorgeschlagenen § 20 Abs. 4 und 5 DSt darf zunächst auf die Ausführungen zum vorgeschlagenen § 84 GOG verwiesen werden. Eine der dort näher beschriebenen „Öffnungsklauseln“ der DSGVO, die den Mitgliedstaaten als fakultative Regelungsspielräume im Anwendungsbereich der Verordnung unter bestimmten Voraussetzungen abweichende oder auch den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten, betrifft (auch) den Bereich des anwaltlichen (wie auch des notariellen) Disziplinarrechts.

Konkret sind nach Art. 23 Abs. 1 lit. g DSGVO Beschränkungen der in den Art. 12 bis 22 und Art. 34 sowie Art. 5 DSGVO vorgesehenen Rechte und Pflichten im Weg von Gesetzgebungsmaßnahmen dann zulässig, wenn die Beschränkung der Sicherstellung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe dient. Erforderlich ist ferner, dass die Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt.

Von dieser Öffnungsklausel soll im Bereich des Verfahrens vor dem Disziplinarrat der Rechtsanwaltskammer und dem Kammeranwalt dahingehend Gebrauch gemacht werden, dass sich die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung nach dem 5. Abschnitt des DSt richten. Daneben bleibt die Zuständigkeit der Datenschutzbehörde als Aufsichtsbehörde unberührt. Ihre Zuständigkeit reicht dabei aber nur so weit, als Rechte und Pflichten des Einzelnen nach der DSGVO bestehen.

Dahinter steht die Überlegung, dass das anwaltliche Disziplinarverfahren auch in erster Instanz besonderen verfahrensrechtlichen Anforderungen gerecht werden muss, um einerseits den – dem übergeordneten Interesse einer geordneten Rechtspflege dienenden – Anspruch auf wirksame Verfolgung von Verstößen gegen das anwaltliche Berufs- und Standesrecht hinreichend zu gewährleisten und andererseits den Vorgaben des Rechts auf ein faires Verfahren gemäß Art. 6 EMRK zu entsprechen.

Unter Beachtung dieser Zielsetzungen enthält das DSt in seinem 5. Abschnitt ein ausgewogenes Regulativ dazu, wie die Ermittlung der für die Beurteilung der an den Kammeranwalt bzw. den Disziplinarrat herangetragenen disziplinarrechtlichen Vorwürfe gegen einen Rechtsanwalt (oder Rechtsanwaltsanwärter) benötigten Daten zu erfolgen hat und wie diese verwendet werden dürfen (vgl. §§ 22 und 27 ff DSt). Ebenso geregelt sind die Informations- und Auskunftsrechte des Beschuldigten (siehe ua. § 22 Abs. 4 und § 27 Abs. 2 DSt) und die Frage (des Umfangs des Rechts) der Akteneinsicht (§ 27 Abs. 5 und § 31 Abs. 3 DSt).

Das verfahrensrechtliche Regime des 5. Abschnitts des DSt entspricht von seinem Wesen und seinem Inhalt her insgesamt den Anforderungen an ein formelles gerichtliches Verfahren; dies wird nicht zuletzt durch die in § 77 DSt ergänzend angeordnete sinngemäß Anwendung von Bestimmungen der StPO deutlich. Dieses Verfahrensrecht regelt dabei die Informations- und Auskunftsrechte, die Frage der Ermittlung und Verarbeitung der Daten und deren Verwendung auf eine Weise, die – unter Berücksichtigung datenschutzrechtlicher Vorgaben – die effektive Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen das Berufs- und Standesrecht der Rechtsanwälte sicherstellt. Es erscheint daher in Anwendung der Öffnungsklausel des Art. 23 Abs. 1 lit. g DSGVO legitim und gerechtfertigt, die (im Sinn der DSGVO) von einem anwaltlichen Disziplinarverfahren betroffene Person zur Durchsetzung ihres Rechts auf Schutz bei der Verarbeitung personenbezogener Daten im Verfahren vor dem Disziplinarrat und dem Kammeranwalt insgesamt auf dieses besondere Regulativ zu verweisen.

Die Umstände können es dabei gerade im Verhältnis zum Beschuldigten auch erfordern, Informationen oder Auskünfte zum Disziplinarverfahren soweit und solange aufzuschieben, einzuschränken oder zu unterlassen, wie dies im Einzelfall zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von Disziplinarvergehen unbedingt erforderlich und verhältnismäßig ist. Zu denken ist dabei etwa an Konstellationen, wo aufgrund entsprechender (frühzeitiger) Bekanntgaben Verdunkelungsgefahr besteht

oder die Sicherstellung von Beweismitteln vereitelt werden könnte. Mit dem – § 43 Abs. 4 DSG idF BG BGBl. I Nr. 120/2017 entsprechenden – vorgeschlagenen § 20 Abs. 5 DSt soll diesem Erfordernis Rechnung getragen werden. Klargestellt sei in diesem Zusammenhang noch, dass der vorgeschlagene Abs. 5 den Regelungsbereich des § 79 DSt unberührt lässt.

Zur Entscheidung über Rechtsmittel gegen Erkenntnisse des Disziplinarrats ist gemäß § 46 DSt der Oberste Gerichtshof zuständig. Da es sich insofern um ein ordentliches gerichtliches Verfahren handelt, erübrigen sich im vorliegenden Kontext gesonderte datenschutzrechtliche Anordnungen dazu im DSt.

Zu Art. 104 (Änderung der EO):

Zu Z 1 und 2 (§ 275 Abs. 6 und § 382g Abs. 1 EO):

In § 275 Abs. 6 und § 382g Abs. 1 Z 4 werden terminologische Anpassungen aus Anlass der Datenschutz-Grundverordnung vorgenommen.

Zu Art. 105 (Änderung des GOG):

Zu Z 1 (§ 16a GOG):

Mit der vorgeschlagenen Bestimmung soll eine ausdrückliche gesetzliche Grundlage für die Veröffentlichung eines sogenannten „Verhandlungsspiegels“ durch die Gerichte geschaffen werden.

Durch die Veröffentlichung eines Verhandlungsspiegels soll es der Bevölkerung erleichtert werden, sich einen Überblick über den Ort, den Tag, die Stunde des Beginns und den Gegenstand des Verfahrens der am jeweiligen Gericht stattfindenden öffentlichen Gerichtsverhandlungen in bürgerlichen Rechtssachen und in Strafsachen zu verschaffen. Mit der vorgeschlagenen Regelung soll klargestellt werden, dass die Allgemeinheit nur über öffentliche Gerichtsverhandlungen entsprechend informiert werden soll.

Ob solche Verhandlungsspiegel überhaupt erstellt und in welcher Form sie von den Gerichten veröffentlicht werden (etwa durch Aushang am „schwarzen Brett“, Darstellung auf einem Infoscreen oder auf der Website des Gerichts), bleibt der Entscheidung der zuständigen Organe der Justizverwaltung überlassen.

Zu Z 2 (§§ 83 bis 85a GOG):

Datenverarbeitungen in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der weisungsfreien Justizverwaltung fallen in den Anwendungsbereich der DSGVO, die am 25.5.2018 in Geltung tritt.

Datenverarbeitungen in Angelegenheiten der Strafgerichtsbarkeit fallen in den Anwendungsbereich der Richtlinie (EU) 2016/680 (im Folgenden: DS-RL), die mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, umgesetzt wurde, welches gemeinsam mit der DSGVO in Kraft treten wird.

Demnach ist es erforderlich, die bestehenden datenschutzrechtlichen Regelungen der §§ 83 bis 85 GOG an die (teilweise) neuen rechtlichen Gegebenheiten und Instrumentarien der DSGVO und des DSG für den Bereich der Datenverarbeitungen in Angelegenheiten der Gerichtsbarkeit anzupassen.

Da nun nicht mehr – wie bisher mit dem DSG 2000 – ein einheitliches datenschutzrechtliches Regelungswerk besteht, ist es erforderlich, in Anpassung an die rechtlichen Vorgaben der DSGVO und des neuen Datenschutzgesetzes getrennte Regelungen für die Gerichtsbarkeit in bürgerlichen Rechtssachen und der weisungsfreien Justizverwaltung einerseits (§§ 83 bis 85 des Entwurfs) sowie für Angelegenheiten der Strafgerichtsbarkeit andererseits (§ 85a des Entwurfs) vorzusehen.

Zu § 83 GOG:

Nach dem vorgeschlagenen § 83 Abs. 1 dürfen die Gerichte im Rahmen ihrer justiziellen Tätigkeit die hiefür erforderlichen personenbezogenen Daten verarbeiten.

Diese generelle Festlegung trägt dem sowohl im innerstaatlichen wie auch im europäischen Datenschutzrecht geltenden Prinzip Rechnung, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, wenn der Gesetzgeber nicht ausdrücklich eine Erlaubnis erteilt. Die näheren Umstände, welche Daten für welche Zwecke und in welchem Umfang von den Gerichten ermittelt und auf welche Weise diese verarbeitet werden dürfen, sowie alle weiteren für die gerichtlichen Datenverarbeitungen geltenden Grundsätze werden durch die von den Gerichten einzuhaltenden Verfahrensgesetze und den darauf beruhenden Verordnungen sowie die Vorschriften des GOG determiniert. Dabei wird in Hinkunft auch Art. 5 DSGVO als Leitlinie für die (europarechtskonforme) Auslegung der nationalen Bestimmungen dienen.

Der bereits im vorgeschlagenen § 83 Abs. 1 verwendete Begriff der „justiziellen Tätigkeit“ der Gerichte soll im vorgeschlagenen § 83 Abs. 2 definiert werden. Dieser Begriff wird in der DSGVO im Zusammenhang mit den Bereichsausnahmen der Artikel 37 Abs. 1 lit. a (Benennung eines

Datenschutzbeauftragten) und Artikel 55 Abs. 3 (Aufsichtsbehörden) verwendet. In Erwägungsgrund 20 der DSGVO wird damit im Zusammenhang ausgeführt, dass die Aufsichtsbehörden (in Österreich: die Datenschutzbehörde) nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein sollen, damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassungen unangetastet bleibt.

Im Sinne dieses Begriffsverständnisses, welches ausdrücklich den Schutz der Unabhängigkeit der Justiz und den Begriff der justiziellen Tätigkeit der Gerichte in einen Bedeutungszusammenhang stellt, wird im vorgeschlagenen § 83 Abs. 2 festgelegt, dass die justizielle Tätigkeit der Gerichte alle Tätigkeiten umfasst, die zur Erfüllung der Aufgaben in Angelegenheiten der ordentlichen Gerichtsbarkeit erforderlich sind.

Durch die Formulierung „in Angelegenheiten der ordentlichen Gerichtsbarkeit“ soll deutlich gemacht werden, dass der Anwendungsbereich des vorgeschlagenen § 83 – ebenso wie dies beim geltenden § 83 GOG der Fall ist – nicht nur die gerichtliche Entscheidungstätigkeit als Kernbereich der unabhängigen Rechtsprechung umfassen soll, sondern auch die in Senaten ausgeübte Justizverwaltung, die ebenfalls als Gerichtsbarkeit im formellen Sinn zu betrachten ist. Sofern Aufgaben der Justizverwaltung kollegial zu besorgen sind, werden die Richter in Ausübung ihres richterlichen Amtes tätig und liegt eine Vollziehung durch Gerichtsbehörden vor (vgl. Art. 87 Abs. 2 B-VG; VfSlg. 7753/1976, 13.215/1992, 19.618/2012).

Ebenso Teil der justiziellen Tätigkeit der Gerichte sind die Aufgaben und Befugnisse, die im Zusammenhang mit dem Verlassenschaftsverfahren den Notaren in ihrer Funktion als Gerichtskommissäre gesetzlich zugewiesen sind. Auch die Befundaufnahme und Gutachtenserstattung der gerichtlich bestellten Sachverständigen ist Teil des gerichtlichen Beweisverfahrens und gehört somit in diesem Umfang zur justiziellen Tätigkeit der Gerichte.

Soweit die Tätigkeit der Justizverwaltung nicht in Senaten vollzogen wird, ist diese nicht als justizielle Tätigkeit der Gerichte im Sinn der DSGVO und des vorgeschlagenen § 83 Abs. 2 GOG zu qualifizieren.

Zu § 84 GOG:

Die DSGVO und das DSG nehmen die Tätigkeit der Justiz nicht generell von ihrem sachlichen Anwendungsbereich aus. Die datenschutzrechtlichen Vorgaben der DSGVO und des DSG gelten demnach grundsätzlich für jegliches im Zusammenhang mit einem zivilgerichtlichen Verfahren oder der Tätigkeit in Angelegenheiten der Justizverwaltung ermitteltes personenbezogenes Datum, welches elektronisch (in der Verfahrensautomation Justiz oder in Hinkunft im System Justiz 3.0) gespeichert wird. Die DSGVO enthält jedoch sogenannte „Öffnungsklauseln“, also fakultative Regelungsspielräume, die den Mitgliedstaaten im sachlichen Anwendungsbereich der Verordnung abweichende oder in bestimmten Bereichen den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten.

In diesem Sinn legt Art. 23 DSGVO nähere Voraussetzungen für allfällige Beschränkungen der Betroffenenrechte gemäß den Art. 12 bis 22 und 34 DSGVO in konkreten Konstellationen sowie Vorgaben in Bezug auf die gesetzliche Ausgestaltung fest. Sieht das nationale Recht derartige Beschränkungen vor, so müssen diese Regelungen den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Solche Beschränkungen sind überdies nur zur Sicherstellung bestimmter, in den in Art. 23 Abs. 1 lit. a bis j DSGVO angeführter Schutzzwecke zulässig, so etwa zum Schutz der Unabhängigkeit der Justiz und zum Schutz von Gerichtsverfahren (lit. f).

Die in den Art. 12 bis 22 und 34 DSGVO angeführten Datenschutzrechte des Einzelnen, die in obigem Sinn gesetzlich eingeschränkt werden können, betreffen etwa das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung. In ähnlicher Weise ermöglicht § 1 Abs. 4 DSG bei Eingriffen staatlicher Behörden zur Wahrung überwiegender berechtigter Interessen eines anderen gesetzliche Beschränkungen der Rechte auf Auskunft, Richtigstellung und Löschung gemäß § 1 Abs. 3 DSG, wenn diese den Voraussetzungen des § 1 Abs. 2 DSG genügen, also insbesondere aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind, und der Eingriff verhältnismäßig ist.

Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Tätigkeit der ordentlichen Gerichtsbarkeit erfordern es, dass von der genannten Öffnungsklausel des Art. 23 DSGVO bzw. § 1 Abs. 4 DSG Gebrauch gemacht wird, um die Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren zu gewährleisten. Der dabei im vorgeschlagenen § 84 verfolgte Grundgedanke lautet, dass sich bei Datenverarbeitungen im Rahmen der justiziellen Tätigkeit in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der in Senaten zu erledigenden Justizverwaltung die sich aus Art. 12 bis 22 und Art. 34 DSGVO und die sich aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung nach den

Verfahrensgesetzen und den darauf beruhenden Verordnungen sowie den Vorschriften des GOG richten. Diese Abgrenzung entspricht auch der derzeitigen Rechtslage und Judikatur zum Datenschutz in Angelegenheiten der Gerichtsbarkeit gemäß §§ 83 bis 85 GOG in der derzeit geltenden Fassung.

Die im Gerichtsverfahren (insbesondere im Beweisverfahren) notwendige Verwendung von Daten muss speziellen Zielsetzungen gerecht werden. Die Gerichtsbarkeit in bürgerlichen Rechtssachen muss den Rechtsverfolgungsanspruch und gleichzeitig den Rechtsverteidigungsanspruch der Parteien unter Beachtung der Vorgaben des Rechts auf ein faires Verfahren gemäß Art. 6 EMRK wahren. Dritte Personen dürfen nur ausnahmsweise und in speziell geregelten Konstellationen Einblick in die Verfahrensinhalte bekommen. Rechtsfürsorgeverfahren, wie etwa im Bereich der Erwachsenenschutz- oder Kindschaftsverfahren, verfolgen hingegen andere Verfahrenszwecke und stellen die Interessen der schutzberechtigten Personen in den Vordergrund. Es erfordert daher ein ausdifferenziertes und auf die Bedürfnisse der jeweiligen Verfahrensart abgestelltes Regulativ, welche Daten vom Gericht ermittelt und wie diese verwendet werden dürfen. Die entsprechenden gesetzlichen Grundlagen finden sich in den maßgebenden Verfahrensgesetzen (insbesondere ZPO, AußStrG und JN), in den darauf beruhenden Verordnungen (insbesondere in der Geo.) sowie im GOG. Diese Bestimmungen nehmen, sofern sie die Rechte und Pflichten gemäß den Art. 12 bis 22 und 34 DSGVO sowie § 1 Abs. 3 DSG (teilweise) beschränken, die von Art. 23 Abs. 2 DSGVO und § 1 Abs. 2 DSG geforderten Wertungen und Abwägungen vor.

Die gerichtlichen Verfahrensgesetze, die darauf basierenden Verordnungen und das GOG regeln die datenschutzrechtlichen Rechte und Pflichten für den Bereich der Gerichtsverfahren abschließend.

Derselbe Grundsatz gilt für die Angelegenheiten der in Senaten zu erledigenden Justizverwaltung. Auch bei diesen Agenden der unabhängigen richterlichen Tätigkeit müssen spezifische Verfahrenszwecke gewahrt werden, weshalb ein abweichendes datenschutzrechtliches Regulativ auch in diesem Bereich erforderlich ist. Zu diesen Angelegenheiten zählen etwa die Geschäftsverteilung für die gerichtlichen Geschäfte, die Besetzungsvorschläge für die ausgeschriebenen Richterplanstellen und die Dienstbeschreibungen der Richter (vgl. *Fellner/Nogratnig*, RStDG – GOG[4] [2015] § 31 GOG Anm 6).

Die Verfahrensgesetze gestalten somit die Rechte auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung auf eine Art und Weise, die – unter Berücksichtigung datenschutzrechtlicher Vorgaben – das Funktionieren und die Unabhängigkeit der Gerichtsbarkeit sicherstellen. In manchen Bereichen gehen die durch die Verfahrensgesetze eingeräumten Rechte über die von der DSGVO eingeräumten hinaus, in manchen Bereichen sind sie nur anders gestaltet und in anderen Bereichen wiederum eingeschränkt oder ausgeschlossen.

So sind beispielsweise Parteien und Zeugen grundsätzlich verpflichtet, im gerichtlichen Verfahren Auskunft über personenbezogene Daten zu erteilen. Zur Gewährleistung bestimmter überwiegender persönlicher Interessen an der Geheimhaltung bestimmter Informationen enthalten die Verfahrensgesetze detaillierte Regelungen, unter welchen Voraussetzungen bzw. in welchem Umfang Parteien oder Zeugen – zur Wahrung auch ihres datenschutzrechtlichen Widerspruchsrechts – die Beantwortung von Fragen verweigern dürfen (so die §§ 321 ff, § 380 ZPO, die gemäß § 35 AußStrG auch im außerstreitigen Verfahren anzuwenden sind).

Für die Frage, unter welchen Umständen der Gegenpartei oder einem Dritten die Vorlage von Urkunden aufgetragen werden kann, enthalten die (gemäß § 35 AußStrG auch im außerstreitigen Verfahren anwendbaren) §§ 298 ff ZPO detaillierte Regelungen, deren Einhaltung die entsprechenden Anordnungen des Gerichtes auch datenschutzrechtlich absichert.

Anstelle des datenschutzrechtlichen Auskunfts- und Informationsrechts steht den Parteien das Recht auf Akteneinsicht zu. Das über das Recht auf Akteneinsicht Erlangbare geht weit über den Umfang jener Information hinaus, die im Wege der datenschutzrechtlichen Auskunfts- und Informationserteilung zu erzielen ist. Da die Gerichte in erster Linie personenbezogene Daten der Verfahrensparteien verarbeiten, werden die datenschutzrechtlichen Vorgaben für den Großteil der von der Gerichtsbarkeit verarbeiteten Daten in diesem Bereich übererfüllt. Die grundsätzlich in jeder Phase des Gerichtsverfahrens zu wahrende Parteiöffentlichkeit gewährleistet somit das datenschutzrechtliche Informations- und Auskunftsrecht.

Lediglich das Recht dritter Personen, deren Daten Eingang in Gerichtsverfahren finden, wie Zeugen, Dolmetscher oder Sachverständiger, auf Auskunft und Information ist nur eingeschränkt gegeben. Ihnen stehen Akteneinsichtsrechte nur soweit zu, als sie auch Parteistellung haben (zB bei Verhängung von Ordnungsstrafen gegen Zeugen oder bei Bestimmung der Gebühren des Sachverständigen) oder ein rechtliches Interesse dartun können. Die verarbeiteten Daten der Parteien sollen nicht oder nur im unbedingt nötigen Ausmaß für andere Personen zugänglich sein. § 219 ZPO sieht daher nur für die

Parteien des Verfahrens ein uneingeschränktes Recht auf Akteneinsicht vor. Fehlt eine Zustimmung der Parteien, so können Dritte nur insoweit Akteneinsicht erlangen, als sie ein rechtliches Interesse glaubhaft machen. Es ist im Einzelfall zu prüfen, ob die Akteneinsicht unbedingt nötig ist oder ob sie einen unverhältnismäßigen Eingriff in Geheimhaltungsrechte anderer im Akt aufscheinender Personen darstellt, wobei bei dieser Abwägung auch die Geheimhaltungsinteressen im Akt aufscheinender (anderer) Dritter zu berücksichtigen sind.

Soweit in besonderen Konstellationen Auskunftsrechte zur Wahrung von Geheimhaltungsinteressen bzw. zur Geltendmachung von Verletzungen des Grundrechts auf Datenschutz erforderlich sind, sollen diese durch Sonderregeln geschaffen werden. So sieht etwa § 6a Grundbuchsumstellungsgesetz einen eigenen Auskunftsanspruch über Abfragen aus dem Personenverzeichnis des Grundbuchs vor, ebenso § 430 EO über Abfragen aus bestimmten Daten aus einem Exekutionsverfahren (tritt mit 1. Jänner 2019 in Kraft).

Das Recht auf Richtigstellung und Löschung ist eng an den Zweck der Datensammlung gebunden: für die Beurteilung, ob ein in einem Register, Geschäftsbehelf oder Gerichtsakt enthaltenes Datum „richtig“ oder „unrichtig“, „zulässig“ oder „unzulässig“ ist, ist nämlich nicht auf seine „objektive“ Richtigkeit, sondern auf den Zweck und die vorhersehbare Verwendung der Datensammlung abzustellen. Ein Recht auf Richtigstellung von personenbezogenen Daten besteht im Zusammenhang mit gerichtlichen Verfahren daher nur ausnahmsweise (etwa im Antrag auf Richtigstellung der Parteibezeichnung, auf Berichtigung einer Entscheidung oder den Vorschriften zur Richtigstellung des gerichtlichen Protokolls). Gerade im Beweisverfahren ermittelte Daten müssen in der Weise, wie diese in das Verfahren Eingang gefunden haben, auch zum Akteninhalt gemacht werden. Selbst falsche Angaben zu Personen können für das Gerichtsverfahren von Relevanz sein und dürfen daher nicht nachträglich einer „Korrektur“ zugänglich sein.

Die Regeln der §§ 173 ff Geo. zur Aktenvernichtung legen fest, welche Akteninhalte zu welchem Zeitpunkt zu löschen sind. Sie gewährleisten dadurch das datenschutzrechtliche Recht auf Löschung.

Was die öffentlichen Bücher (Register), insbesondere Grund- und Firmenbuch, betrifft, so sind die durch die vorgeschlagene Bestimmung getroffenen Abweichungen von den Rechten und Pflichten der Art. 12 bis 22 und 34 DSGVO zum Schutz der betreffenden Gerichtsverfahren und der Unabhängigkeit der Justiz wie folgt zu begründen:

Das Grundbuch ist ein von den Bezirksgerichten in ihrer justiziellen Tätigkeit geführtes öffentliches Verzeichnis, in das Grundstücke und die an ihnen bestehenden dinglichen Rechte eingetragen werden. Es dient der Sicherung des Rechtsverkehrs durch Offenkundigkeit der Rechtsverhältnisse. Dingliche Rechte an Liegenschaften können – von einigen Ausnahmen abgesehen – nur durch Eintragung in das Grundbuch erworben werden. Das Vertrauen des gutgläubigen rechtsgeschäftlichen Erwerbers auf die Richtigkeit und Vollständigkeit des Grundbuchs ist geschützt.

Daraus folgt zum einen, dass die in das Grundbuch eingetragenen personenbezogenen Daten jedermann zur Einsicht offenstehen müssen. Das Grundbuchsumstellungsgesetz sieht eine Einschränkung dieses Grundsatzes nur insofern vor, als es für die Einsicht in das Personenverzeichnis ein rechtliches Interesse verlangt.

Darüber hinaus muss aus der Einsicht in das Grundbuch auch die Kette der Rechtserwerbe und Rechtsverluste lückenlos nachvollziehbar sein. Nicht mehr aktuelle oder zu berichtigende ursprünglich unrichtige Grundbuchseintragungen werden aus diesem Grund nur im Hauptbuch gelöscht und in das Verzeichnis der gelöschten Eintragungen (§ 3 GUG) aufgenommen, das dem Hauptbuch gleichsteht und wie dieses von jedermann einsehbar ist.

Das – aus dem Hauptbuch und der Urkundensammlung bestehende – Firmenbuch wird von den Gerichten in ihrer justiziellen Tätigkeit geführt (vgl. § 7 UGB) und dient der Offenlegung von Tatsachen, die nach dem Firmenbuchgesetz (FBG) oder nach sonstigen gesetzlichen Vorschriften einzutragen sind (vgl. § 1 Abs. 2 FBG). Es ist gesetzlich genau festgelegt, welche Rechtsträger in das Firmenbuch einzutragen sind, welche Angaben die Eintragungen zu enthalten haben und welche Urkunden in die Urkundensammlung aufzunehmen sind. Für Kapitalgesellschaften ist die Offenlegung von bestimmten Urkunden und Angaben in einem öffentlichen Register auch unionsrechtlich geboten (vgl. Art. 14 ff der Richtlinie 2017/1132 über bestimmte Aspekte des Gesellschaftsrechts).

Eintragungen in das Firmenbuch erfolgen in aller Regel auf Antrag. Dabei kann die Identität des Antragstellers verlässlich geprüft werden, weil die Unterschrift des Antragstellers grundsätzlich der gerichtlichen oder notariellen Beglaubigung bedarf (vgl. § 11 Abs. 1 UGB). Teilweise bestehen auch für die der Anmeldung zugrundeliegenden Rechtsgeschäfte (z. B. den Abschluss eines Gesellschaftsvertrags) besondere Formpflichten (z. B. Notariatsaktsform), was eine verlässliche Dokumentation der Vorgänge und eine Vorabprüfung ihrer Rechtmäßigkeit gewährleistet.

Das Firmenbuchgericht ist zu einer genauen Prüfung der Anmeldung und ihrer Beilagen verpflichtet und darf eine Eintragung im Firmenbuch nur vornehmen, wenn alle formellen und materiellen Voraussetzungen erfüllt sind. Die maßgeblichen Verfahrensvorschriften finden sich im FBG, das in seinem § 15 Abs. 1 auch eine subsidiäre Geltung des AußStrG anordnet. Demnach liegt jeder Eintragung ein entsprechender Beschluss des Firmenbuchgerichts zugrunde, gegen den gegebenenfalls ein Rechtsmittel (Rekurs) erhoben werden kann. Von vornherein unzulässige oder unzulässig gewordene Eintragungen kann das Gericht auch von Amts wegen löschen (vgl. § 10 Abs. 2 FBG).

Ändert sich eine im Firmenbuch eingetragene Tatsache, so ist der Rechtsträger zur unverzüglichen Anmeldung dieser Änderung verpflichtet (vgl. § 10 Abs. 1 FBG). Diese Verpflichtung kann – wie alle Verpflichtungen zur Vornahme einer Anmeldung oder Einreichung zum Firmenbuch – mit einer vom Firmenbuchgericht zu verhängenden Zwangsstrafe durchgesetzt werden. Dadurch wird gewährleistet, dass gesetzlich vorgeschriebene Anmeldungen auch tatsächlich vorgenommen werden.

Zu § 85 GOG:

Der vorgeschlagene § 85 GOG entspricht im Wesentlichen der geltenden Bestimmung.

Mit der vorgeschlagenen Fassung wird die Bestimmung im Hinblick auf § 85a GOG des Entwurfs, welcher nunmehr den Rechtsschutz bei Verletzungen im Grundrecht auf Datenschutz in Angelegenheiten der Strafgerichtsbarkeit regelt, lediglich in ihrem Anwendungsbereich auf Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der – nunmehr auch ausdrücklich angeführten – weisungsfreien Justizverwaltung beschränkt.

Außerdem wird die Bestimmung begrifflich an die Terminologie der DSGVO („justizielle Tätigkeit“) angepasst.

Zu § 85a GOG:

Die Zulässigkeit der Verarbeitung von Daten durch Strafgerichte richtet sich grundsätzlich nach den Bestimmungen der StPO. Eine § 83 Abs. 1 GOG entsprechende ausdrückliche gesetzliche Grundlage der Berechtigung zur Verarbeitung soll in § 74 Abs. 1 StPO aufgenommen werden, um nicht nur Gerichte, sondern auch Staatsanwaltschaft und Kriminalpolizei zu erfassen.

Dem Begriff Angelegenheiten der Strafgerichtsbarkeit liegt ein weites Verständnis zugrunde. So ist eine Verarbeitung personenbezogener Daten nicht nur im Bereich der gerichtlichen Entscheidungstätigkeit, sondern auch in jenem der zur unabhängigen Rechtsprechung zählenden kollegialen Justizverwaltung (Art. 87 Abs. 2 B-VG) unter den durch § 74 Abs. 2 StPO normierten Prämissen zulässig. Ebenso erfasst ist die Tätigkeit der im Gerichtsverfahren bestellten Sachverständigen und Dolmetscher.

Einer § 84 GOG idgF entsprechenden Bestimmung bedarf es für den Bereich der Strafgerichtsbarkeit nicht. Die den angeführten Bestimmungen der Verordnung (EU) 2016/679 entsprechenden Regelungen der DS-RL wurden im Wesentlichen durch §§ 43 bis 45 DSG idF BGBl. I. Nr. 120/2017 umgesetzt. Sie umfassen die Verpflichtung des Verantwortlichen zur Information sowie die Rechte der betroffenen Person auf Auskunft, Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung. Hierbei handelt es sich um Pflichten bzw. Rechte, hinsichtlich derer spezielle, auf die besondere Stellung und Funktion des Strafverfahrens abstellende Regelungen in der StPO bestehen. Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (leges speciales) den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. So sind etwa insbesondere die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten als leges speciales zum 3. Hauptstück des DSG zu betrachten. Informationsverpflichtungen sind etwa in § 50, § 138 Abs. 5, § 139 Abs. 2 StPO zu ersehen, wobei diese im Einklang mit der für das Strafverfahren wesensimmanenten Zielsetzung der Aufklärung von Straftaten und Verfolgung verdächtiger Personen (§ 1 Abs. 1 StPO) unter Wahrung der Rechte Verdächtiger bzw. Beschuldigter auch dem Umstand einer möglichen Gefährdung des Zwecks des strafrechtlichen Ermittlungsverfahrens Rechnung tragen. Die Auskunft innerhalb der StPO wird typischerweise über die Regelung der Akteneinsicht präzisiert. Daneben bleibt kein Raum für das Auskunftsrecht nach dem DSG (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 60). In diesem Sinn führt auch der Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 23 aus, dass § 44 Abs. 5 DSG idF BGBl. I. Nr. 120/2017 die bisherige Regelung des § 26 Abs. 8 DSG 2000 übernimmt, wodurch klargestellt wird, dass das Auskunftsrecht wie bisher nicht zur Umgehung von in Materiengesetzen geregelten speziellen Einsichtsrechten (z. B. Akteneinsicht) herangezogen werden kann. In § 75 StPO finden sich ferner ausdrückliche Vorschriften über das Berichtigen, Löschen und Sperren personenbezogener Daten. Dort, wo es an entsprechenden Regelungen in der StPO fehlt, finden gemäß § 74 Abs. 1 StPO die Bestimmungen des DSG subsidiär im Strafverfahren Anwendung.

§ 85 GOG kommt aufgrund seiner Ausgestaltung als subsidiärer Rechtsschutz nur dort zum Tragen, wo die StPO für die Durchsetzung der Datenschutzrechte keine ausreichenden Instrumente vorsieht. Der Anwendungsbereich der Bestimmung ist im Strafverfahren daher denkbar klein, weil typischerweise nach der StPO mit Einspruch wegen Rechtsverletzung, Beschwerde oder Nichtigkeitsbeschwerde/Berufung gegen das Urteil vorgegangen werden kann, um Datenschutzverletzungen geltend zu machen. Erst wo diese Möglichkeiten enden, ist das GOG einschlägig (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 67). Die durch das Strafprozessrechtsänderungsgesetz 2013, BGBl. I Nr. 195/2013, entfallene Befristung der Einbringungsmöglichkeit eines Einspruchs wegen Rechtsverletzung gemäß § 106 StPO mit Beendigung des Ermittlungsverfahrens hat zu einer weiteren Verkleinerung des Anwendungsbereichs des § 85 GOG geführt. Dessen ungeachtet dient die Bestimmung (etwa im Bereich der Geschäftsregister) nach wie vor dazu, dort Lücken im Rechtsschutz zu schließen, wo die Verfahrensordnung einen solchen nicht bietet. Aus diesem Grund wird die Geltung des § 85 GOG auch auf Strafgerichte erweitert.

Zu Z 3, 6 und 7 (Überschriften der §§ 89f, 89g und 89i GOG):

Da die jeweils vorangehenden Überschriften (vor § 89e [„Haftung für IT-Einsatz“] und § 89h [„Amtshilfe der Sozialversicherungsträger“]) nur für den unmittelbar nachfolgenden Paragraphen passen, sollen §§ 89f, 89g und 89i zu ihrem Inhalt passende Überschriften erhalten.

Zu Z 4 und 5 (§ 89f GOG):

Die vorgeschlagenen Regelungen betreffen terminologische Anpassungen an die DSGVO. Das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz ist als Verantwortlicher für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten im Justizressort – neben der Abwicklung des Strafvollzuges und der Führung der zivil- und strafgerichtlichen Verfahren zählen hierzu nun insbesondere auch die vor dem Bundesverwaltungsgericht geführten Verfahren – verantwortlich. Es hat insbesondere sicherzustellen, dass die Sicherheit und Vertraulichkeit von personenbezogenen Daten hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können (Art. 5 DSGVO). Die hierzu erforderlichen technischen und organisatorischen Rahmenbedingungen sind der Bundesrechenzentrum GmbH als Auftragsverarbeiterin nach den Erfordernissen des Einzelfalls, insbesondere nach Maßgabe der Art der verarbeiteten personenbezogenen Daten und dem Einsatzgebiet der Verarbeitungstätigkeit, vom Verantwortlichen vorzugeben.

Zu Z 8 (§§ 89p und 89q GOG):

Zu § 89p GOG:

Die Gerichte dürfen im Rahmen ihrer justiziellen Tätigkeit die hiefür erforderlichen personenbezogenen Daten nach den Vorgaben der Verfahrensgesetze verarbeiten. Ergänzend dazu legen die maßgeblichen Rechtsvorschriften etwa zur Akten- und Registerführung und zu den hiefür bereitgestellten technischen Applikationen (derzeit die Verfahrensautomation Justiz [VJ]) die zulässigen Mittel der Verarbeitung fest.

Auf Basis des Art. 4 Z 7 zweiter Satzteil DSGVO obliegt es dem nationalen Gesetzgeber, in diesen Fällen den jeweils zuständigen Verantwortlichen zu definieren.

Mit dem vorgeschlagenen § 89p wird zunächst zum Ausdruck gebracht, dass im Rahmen der justiziellen Tätigkeit in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der in Senaten zu erledigenden Justizverwaltung das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz und das jeweils verfahrensführende Gericht als für die Verarbeitung Verantwortliche zu betrachten sind. Geregelt wird auch die Aufgabenverteilung der datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitung. Soweit nicht gesondert eine gerichtliche Zuständigkeit vorgesehen ist, treffen die Rechte und Pflichten des Verantwortlichen das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. Diese (Auffang-)Zuständigkeit ergibt sich aus dem Umstand, dass die technische Struktur der von den verfahrensführenden Gerichten verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellten Applikationen (derzeit die Verfahrensautomation Justiz [VJ]) vorgegeben wird. Demnach sollen die Pflichten des Verantwortlichen im Umfang der Vorgaben der DSGVO (etwa gemäß Art. 24, 25 sowie 28 ff DSGVO) das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz treffen.

Entsprechend der im vorgeschlagenen § 84 GOG getroffenen Einschränkung der Anwendbarkeit der Art. 12 bis 22 und 34 DSGVO kommt eine Aufgabenverteilung für diesen Bereich nicht mehr in Frage, weil hier bereits die Verfahrensvorschriften entsprechende (gerichtliche) Zuständigkeiten vorsehen. Daneben sehen die Verfahrensgesetze und das GOG punktuell eigene Zuständigkeiten für Auskunftsrechte außerhalb eines konkreten gerichtlichen Verfahrens vor. So ermöglicht etwa § 89l jedermann beim Bezirksgericht seines Wohnsitzes oder Aufenthalts ein Auskunftsrecht über Gericht und

Aktenzahl aller im elektronischen Register enthaltenen zivilgerichtlichen Verfahren, in denen er Partei ist. Auch hier sieht das jeweilige Materiengesetz eine entsprechende (gerichtliche) Zuständigkeit vor.

Zu § 89q GOG:

Nach § 36 Abs. 2 Z 8 DSG idF BGBl. I. Nr. 120/2017 ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff ersetzt jenen des Auftraggebers nach § 4 Abs. 4 DSG 2000. Der Verantwortliche zeichnet für die Einhaltung der durch §§ 74 f StPO bzw. § 37 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 festgelegten Kriterien der Zulässigkeit einer Datenverarbeitung verantwortlich, ihn treffen unter Berücksichtigung der durch die StPO (das DSG) normierten Voraussetzungen die Pflichten zur Information, Auskunftserteilung, Berichtigung und Löschung personenbezogener Daten und Einschränkung deren Verarbeitung.

Nach Art. 3 Z 8 DS-RL gilt, dass für den Fall, dass die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind, der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden können. Die (Straf-)Gerichte dürfen die für die Ausübung ihrer Aufgaben erforderlichen personenbezogenen Daten nach den Vorgaben der Verfahrensgesetze, welche Zweck und Mittel der jeweils rechtmäßigen Datenverarbeitung im Gerichtsverfahren bestimmen, verarbeiten. Ergänzend dazu legen die maßgeblichen Rechtsvorschriften etwa zur Akten- und Registerführung und zu den hiefür bereitgestellten technischen Applikationen (derzeit die Verfahrensautomation Justiz [VJ]) die zulässigen Mittel der Verarbeitung fest.

Aufgrund des Umstands, dass die Struktur der seitens des jeweils verfahrensführenden Gerichts verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellte Applikation Verfahrensautomation Justiz (VJ) vorgegeben wird, sollen das jeweils fallbearbeitende Gericht und das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz die Position des Verantwortlichen wahrnehmen. Die Wahrnehmung der Rechte und Pflichten des Verantwortlichen nach der StPO (aufgrund des Verweises in § 74 Abs. 1 StPO subsidiär des DSG) soll dabei ausschließlich das jeweils verfahrensführende Gericht treffen. Zur Vermeidung der Notwendigkeit einer Befassung jedes einzelnen in Strafsachen tätigen Gerichts soll im Einklang mit der für den zivilgerichtlichen Bereich geltenden Bestimmung des § 89l GOG festgelegt werden, dass jede auskunftssuchende Person beim Haft- und Rechtsschutzrichter des für Strafsachen zuständigen Landesgerichts seines Wohnsitzes oder gewöhnlichen Aufenthalts eine bundesweite Auskunft über Gericht und Aktenzahl aller in der VJ enthaltenen strafgerichtlichen Haupt- und Rechtsmittelverfahren beantragen kann, in denen sie Beteiligte ist. Eine Auskunft über anhängige Ermittlungsverfahren darf jedoch selbst für den Fall, dass in einem solchen Verfahren eine Befassung des Haft- und Rechtsschutzrichters erfolgt ist, nicht erteilt werden, weil diese Verfahren unter Leitung der Staatsanwaltschaft – und nicht des Gerichts – stehen (§ 20 Abs. 1 StPO).

Zu Z 9 und 10 (§§ 91b und 91d GOG):

Die vorgeschlagenen Regelungen betreffen terminologische Anpassungen an die DSGVO.

Zu Z 11 (Inkrafttretens- und Übergangsbestimmungen)

Die Änderungen sollen gleichzeitig mit dem Inkrafttreten der DSGVO in Kraft treten. Übergangsbestimmungen sind lediglich für die §§ 84, 85 und 85a erforderlich.

Zu Art. 106 (Änderung des GUG):

Zu Z 1 (§ 6a GUG):

Rechtsanwälte und Notare sind gemäß § 6 Abs. 2 GUG unter bestimmten Umständen zur direkten Abfrage des Personenverzeichnisses befugt: Notare, um als Gerichtskommissär in Verlassenschaftssachen oder als Erbenmachthaber verbücherte Rechte des Erblassers zu ermitteln (Z 1); Rechtsanwälte, um als Erbenmachthaber verbücherte Rechte des Erblassers zu ermitteln und um Personen, die im Personenverzeichnis eingetragen sind, Abschriften und Mitteilungen über die sie betreffenden Eintragungen zu erteilen (Z 1a); Notare und Rechtsanwälte, um als Vertreter des Gläubigers einer vollstreckbaren Geldforderung verbücherte Rechte des Schuldners zu ermitteln (Z 1b). In den nach den genannten Bestimmungen nicht vorgesehenen Fällen haben auch Notare und Rechtsanwälte die Einsicht in das Personenverzeichnis nach § 5 Abs. 4 GUG bei Gericht zu beantragen und dafür ein rechtliches Interesse darzulegen.

In technischer Hinsicht gehen die Einsichtsmöglichkeiten der Rechtsanwälte und Notare aber über ihre gesetzlich vorgesehenen Einsichtsrechte hinaus. Der Entwurf sieht daher in der vorgeschlagenen Bestimmung einen Auskunftsanspruch über die Abfrage von Daten aus dem Personenverzeichnis durch

Rechtsanwälte und Notare vor, damit die Betroffenen prüfen können, ob die Direktabfrage ihrer Daten aus dem Personenverzeichnis den Anforderungen des § 6 Abs. 2 GUG entsprach.

Die Auskunft ist beim Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz zu beantragen und von diesem zu erteilen.

Gemäß § 6 Abs. 2 Z 2 GUG sind auch die Dienststellen des Bundes, der Länder und der Gemeinden sowie die Sozialversicherungsträger und der Hauptverband der Sozialversicherungsträger zur Abfrage des Personenverzeichnisses befugt, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben notwendig ist. Die Zulässigkeit dieser Abfragen kann von der Justiz nicht überprüft werden; vielmehr muss dies im jeweiligen Wirkungsbereich der genannten Stellen geschehen. Folglich wird den betroffenen Personen in diesem Bereich ein entsprechendes Auskunftsrecht im GUG nicht eingeräumt.

Zu Art. 107 (Änderung der JN):

Zu Z 1 (§ 37 Abs. 6 JN):

Bei Rechtshilfeersuchen eines ausländischen an ein inländisches Gericht (§§ 38, 39 und 40 JN) ist für den Fall der Verweigerung der Rechtshilfe oder bei sonstigen Meinungsverschiedenheiten zwischen dem ersuchenden und dem ersuchten Gericht ein Regulativ vorgesehen (§ 40 JN). Diesfalls hat auf Begehren des ersuchenden ausländischen Gerichts oder eines anderen hiezu berufenen ausländischen öffentlichen Organs das dem ersuchten Gericht vorgesetzte Oberlandesgericht über die Rechtmäßigkeit der Weigerung oder über den sonstigen Gegenstand der Meinungsverschiedenheit zu entscheiden.

Wird einem Ersuchen einer Staatsanwaltschaft um Amts- oder Rechtshilfe von einem ersuchten Gericht nicht oder nicht vollständig entsprochen, so hat das dem ersuchten Gericht übergeordnete Oberlandesgericht gemäß § 76 Abs. 2a StPO auf Antrag der Staatsanwaltschaft ohne vorhergehende mündliche Verhandlung über die Rechtsmäßigkeit der unterlassenen Amts- oder Rechtshilfe oder über den sonstigen Gegenstand der Meinungsverschiedenheit zu entscheiden.

Bei Streitigkeiten zwischen ersuchendem und ersuchtem (jeweils inländischen) Gericht über die Verweigerung der Rechtshilfe ist jedoch ein gerichtliches Verfahren nach geltendem Recht nicht ausdrücklich vorgesehen.

Mit der vorgeschlagenen Bestimmung soll diese Rechtschutzlücke geschlossen werden, indem in diesen Fällen § 40 JN sinngemäß anzuwenden sein soll. Zur Entscheidung über diese Streitigkeit ist das beiden Gerichten übergeordnete Gericht berufen.

Der rechtliche Charakter der Entscheidung über das zugrunde liegende Rechtshilfeersuchen kommt in der gewählten Verweisungsnorm (anders als in § 47 JN, welcher sich alternativ als mögliche Verweisungsnorm angeboten hätte) passend zum Ausdruck. Die Amtshilfe ist zwar ein Akt der Gerichtsbarkeit (6 Ob 656/84), hat aber bloß internen Charakter; weder die Verfahrensparteien noch das ersuchende Organ haben ein subjektives Recht darauf, dass Amtshilfe geleistet oder verweigert wird oder sind Partei in einem Verfahren zur Erlangung der Amtshilfe (vgl. 10 Ob 28/07a).

§ 40 JN eröffnet in sinngemäßer Anwendung einen direkten Rechtszug auf Antrag des ersuchenden Gerichts an das beiden Gerichten übergeordnete Gericht, und zwar in Form einer Beschwerde sui generis. Mit der Beschwerde sollen in der konkreten Rechtshilfesache strittig gewordene (Verfahrens-)Fragen ausjudiziert werden; diese können die (gänzliche oder teilweise) Verweigerung der Rechtshilfe, die Art ihrer Ausführung oder jede sonstige zwischen ersuchendem und ersuchtem Gericht ausgebrochene Meinungsverschiedenheit betreffen (vgl. *Sengstschmid* in *Fasching/Konecny*[3] § 40 JN Rz 1).

Zu Z 2 (§ 37a JN):

Mit der vorgeschlagenen Bestimmung soll die in der gerichtlichen Praxis ebenfalls immer wieder strittige Frage geklärt werden, in welchen Fällen die von Verwaltungsbehörden (etwa den Gewerbebehörden, Finanzämtern, Kinder- und Jugendhilfeträgern ua) an ein Gericht gestellten Ersuchen um Amtshilfe durch Übersendung des Gerichtsaktes zulässig sind und in welchen Fällen diese verweigert werden dürfen.

Die Aktenübersendung wird als häufigster Fall der – der Rechtshilfe vergleichbaren – Amtshilfe zwischen den Organen der Vollziehung (Art. 22 B-VG) genannt (6 Ob 656/84).

Gemäß Art. 22 B-VG sind alle Organe des Bundes, der Länder und der Gemeinden im Rahmen ihres gesetzmäßigen Wirkungsbereichs zur wechselseitigen Amtshilfe verpflichtet. Zur Möglichkeit der Ausgestaltung dieser Verpflichtung durch einfaches Gesetz führt *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Rz 50 zu Art. 22 B-VG mit Verweis auf mehrere Belegstellen aus, es sei nahezu unbestritten, dass der Gesetzgeber Art. 22 B-VG näher ausgestalten, d.h. die Amtshilfe zwischen Organen und Gebietskörperschaften konkretisieren darf. Dem Gesetzgeber steht daher nicht nur die Erweiterung frei; er kann Amtshilfe auch beschränken (*Wiederin* aaO). Es ist überdies eine

gesetzliche Grundlage in Konstellationen erforderlich, in denen das ersuchte Organ faktische Leistungen erbringen soll, die in Grundrechte eingreifen; Datenübermittlungen, die in Art. 8 EMRK oder in das Grundrecht auf Datenschutz eingreifen, müssen als Informationseingriffe gesetzlich zugelassen sein (*Wiederin* aaO Rz 51).

Vor diesem Hintergrund wird in der vorgeschlagenen Bestimmung die gesetzliche Verpflichtung von Gerichten, Amtshilfe auf Ersuchen inländischer Verwaltungsbehörden durch Übermittlung von Gerichtsakten oder von Teilen dieser zu leisten, dahingehend beschränkt, dass die begehrte Übermittlung nur soweit erfolgen darf, als diese auf einer ausdrücklichen gesetzlichen Grundlage beruht. Die ersuchende Behörde hat die gesetzliche Grundlage für Übermittlung gegenüber dem ersuchten Gericht anzuführen.

Hintergrund dieser Regelung ist, dass es einer ausdrücklich vom jeweiligen Materiengesetzgeber getroffenen Wertungsentscheidung bedarf, in welchen Fällen das Informationsinteresse im Verfahren vor der ersuchenden Behörde das Geheimhaltungsinteresse im gerichtlichen Verfahren überwiegt.

Eine weitere Einschränkung der Verpflichtung zur Amtshilfe kann sich daraus ergeben, dass der Übermittlung bestimmter Informationen aus einem Gerichtsakt spezielle Rechtsvorschriften entgegenstehen, wie dies etwa für Auskünfte über Einkommens- und Vermögensverhältnisse oder Informationen zum Gesundheitszustand der vertretenen Person in Erwachsenenschutzverfahren der Fall ist (vgl. § 141 AußStrG).

Zu Art. 108 (Änderung der Notariatsordnung):

Zu Z 1 (§ 37 Abs. 3a NO):

Das zu § 9 Abs. 3a RAO Gesagte gilt sinngemäß.

Zu Z 2 bis 5 (§§ 55 Abs. 4, 82 Abs. 1 und 113 NO)

Bei der Wahrnehmung der den Notar treffenden Identifizierungspflichten hat dieser auch Ausweis- und (gegebenenfalls) Urkundendaten zu erheben und zu erfassen, die insbesondere beim Notariatsakt auch regelmäßig in der Urkunde selbst angeführt werden. Für eine weitere Verarbeitung dieser Daten sowie deren Anführung im notariellen Beurkundungs- und Geschäftsregister fehlt es bislang aber an einer entsprechenden ausdrücklichen gesetzlichen Grundlage. Eine solche soll mit den zu den §§ 55, 82 und 113 NO vorgeschlagenen Änderungen vorgesehen werden.

Zu Z 6 und 8 (§§ 134 Abs. 4 und 140a Abs. 3 NO):

Die vorgeschlagenen §§ 134 Abs. 4 und 140a Abs. 3 NO sehen – entsprechend den Anforderungen sowohl des europäischen wie auch des österreichischen Datenschutzrechts – vor, dass sowohl die Notariatskammern wie auch die Österreichische Notariatskammer personenbezogene Daten der Notare und Notariatskandidaten, die zur Erfüllung der jeweiligen gesetzlichen Aufgaben der Notariatskammer bzw. der Österreichischen Notariatskammer erforderlich sind, verarbeiten dürfen (wobei sich die Ermächtigung im Bereich der Notariatskammern auf die Daten der Mitglieder des jeweiligen Notariatskollegiums [vgl. § 124 NO], im Bereich der Österreichischen Notariatskammer hingegen auf alle österreichischen Notare und Notariatskandidaten bezieht). Darüber hinaus soll hier auch darauf Bedacht genommen werden, dass die Notariatskammern sowie die Österreichische Notariatskammer im Rahmen ihres jeweiligen gesetzlichen Zuständigkeitsbereichs gegebenenfalls auch Daten von Personen zu verarbeiten haben, die (noch) nicht Standesangehörige sind (ein Beispiel dafür ist etwa die begehrte Eintragung in die Liste der Notariatskandidaten). Durch den Verweis auf Art. 4 Z 2 DSGVO wird gleichzeitig klargestellt, dass unter dem Begriff „verarbeiten“ alle in der genannten Definition der DSGVO angeführten Verarbeitungsvorgänge zu verstehen sind.

Zu Z 7 (§ 140a Abs. 2 Z 11 NO):

Dabei handelt es sich um eine Anpassung an die neue Terminologie der DSGVO.

Zu Z 9 bis 13 (§ 140b Abs. 1 und 7 sowie §§ 140i bis 140k NO):

Die Österreichische Notariatskammer ist gemäß § 140b NO ermächtigt, die darin genannten Register, Archive und Verzeichnisse zu führen.

Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Führung einzelner der Register, Archive und Verzeichnisse gemäß § 140b NO erfordern es, dass (teilweise) von der genannten Öffnungsklausel des Art. 23 DSGVO Gebrauch gemacht wird, um einerseits den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen (Art. 23 Abs. 1 lit. i DSGVO) und andererseits die Durchsetzung zivilrechtlicher Ansprüche (Art. 23 Abs. 1 lit. j DSGVO) zu gewährleisten. Insoweit sollen sich nach der vorgeschlagenen Bestimmung die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG

ergebenden Rechte und Pflichten sowie deren Durchsetzung nach den Vorschriften dieses Bundesgesetzes, des § 91c GOG und der nach § 140a Abs. 2 Z 8 NO erlassenen Richtlinien der Österreichischen Notariatskammer richten, zumal die genannten Vorschriften ein umfassendes und auf die jeweiligen Verarbeitungszwecke abgestimmtes Regulativ (auch der datenschutzrechtlichen Aspekte der betroffenen Register, Archive und Verzeichnisse) vorsehen. Dies betrifft folgende der in § 140b Abs. 1 NO genannten Datenanwendungen:

- das „Österreichische Zentrale Testamentsregister“ (ÖZTR),
- das „Treuhandregister des österreichischen Notariats“ (THR),
- das nach § 91d Abs. 2 GOG hoheitlich zu führende „Urkundenarchiv des österreichischen Notariats“,
- das „Österreichische Zentrale Vertretungsverzeichnis“ (ÖZVV) und
- das „Patientenverfügungsregister des österreichischen Notariats“ (das mit den vorgeschlagenen § 140b Abs. 1 Z 7 und § 140i NO zugleich auf eine eindeutige gesetzliche Grundlage gestellt werden soll).

Das ÖZTR dient der Registrierung der Verwahrung der bei Gerichten, Notaren und Rechtsanwälten hinterlegten letztwilligen Anordnungen, Erbverträge, Vermächtnisverträge, Erb- und Pflichtteilsverzichtsverträge sowie weiteren Urkunden über sonstige Erklärungen auf den Todesfall (§ 140c Abs. 1 NO). Die Österreichische Notariatskammer hat die registrierten Daten bei Anfragen von Verlassenschaftsgerichten und öffentlichen Notaren als Gerichtskommissäre in Verlassenschaftssachen an diese und zu Kontrollzwecken an Gerichte, Notare und Rechtsanwälte auf deren Verlangen hinsichtlich der von ihnen gemeldeten Daten registrierungsfähiger Urkunden zu übermitteln (§ 140c Abs. 3 NO).

Das ÖZTR dient der Auffindbarkeit errichteter Testamente. Bis zum Wirksamwerden des registrierten Testaments dient die Registrierung ausschließlich dem Interesse des Testators. Rechte dritter Personen sind soweit nicht berührt, weshalb diesen auch keine Rechte nach Art. 12 bis 22 und 34 DSGVO zukommen können (und sollen). Mit dem Ableben des Testators ist es Aufgabe der im gerichtlichen Verlassenschaftsverfahren tätigen Organe (Gericht und Gerichtskommissär), allfällige registrierte Testamente abzufordern und gemäß den dann anzuwendenden Verfahrensvorschriften (insbesondere des AußStrG und des GKG) im Rahmen der justiziellen Tätigkeit abzuhandeln; diesfalls kommen die Bestimmungen über das gerichtliche Verfahren zur Anwendung.

Das THR dient der Registrierung der nach § 109a Abs. 2 NO eintragungspflichtigen Treuhandschaften. Einzutragen sind insbesondere der Notar, die Versicherung des Notars, der Treuhandrahmen, die Treugeber und der Beginn und das Ende der Treuhandschaft. Jeder Treugeber ist berechtigt, von der Österreichischen Notariatskammer darüber Auskunft zu verlangen, ob die ihn betreffende Treuhandschaft im THR registriert ist und in welcher Höhe dafür Versicherungsschutz besteht (§ 140d Abs. 1 und 2 NO).

Die §§ 109a und 140d NO und die auf der Grundlage der §§ 109a Abs. 5 und 140b Abs. 2 Z 8 NO ergangenen Richtlinien der Österreichischen Notariatskammer vom 8.6.1999 über die Vorgangsweise bei notariellen Treuhandschaften (THR 1999) enthalten insgesamt ein umfassendes Schutzregime insbesondere zur Absicherung des Treugebers, das auch dessen (über die DSGVO hinausgehenden) Auskunfts- und Informationsrechte im Detail regelt (vgl. etwa die Pkte. 27 ff der THR 1999).

Das Urkundenarchiv des österreichischen Notariats dient der Speicherung von Notariatsakten oder dem Notar von den Parteien übergebenen Urkunden (§ 110 Abs. 1 NO). Zweck des Urkundenarchivs ist ferner die Speicherung von Urkunden, die für den elektronischen Urkundenverkehr mit den Gerichten bestimmt sind.

Das Urkundenarchiv dient insgesamt ausschließlich dem Schutz der Rechte der Parteien und (gegebenenfalls) der Durchsetzung ihrer zivilrechtlichen Ansprüche. Deren datenschutzrechtliche Sphäre ist durch die von der Österreichischen Notariatskammer nach § 140b Abs. 5 NO zu erlassenden Richtlinien sowie die anzuwendenden Verfahrensvorschriften geschützt. Den Parteien ist vom Notar elektronischer Zugang zu diesen Urkunden zu ermöglichen (§ 91c Abs. 3 GOG). Die Parteien sind berechtigt, in der in den Richtlinien vorgesehenen Form auch anderen Personen elektronischen Zugang zu diesen Urkunden einzuräumen. Außer den in diesem Gesetz angeführten Fällen darf ein Zugriff auf diese Urkunden nur über gerichtlichen Auftrag dem Gericht oder im Rahmen der standesrechtlichen Aufsicht über Auftrag der Notariatskammer dieser ermöglicht werden (§ 110 Abs. 3 NO).

Das ÖZVV ist in § 140h NO detailliert geregelt. Es dient insbesondere der Registrierung von Vorsorgevollmachten und (gemäß dem 2. Erwachsenenschutz-Gesetz, BGBl. I Nr. 59/2017, für Eintragungen ab dem 30.6.2018) von Vereinbarungen über eine gewählte Erwachsenenvertretung, von gesetzlichen Erwachsenenvertretungen, Erwachsenenvertreter-Verfügungen und gerichtlichen

Erwachsenenvertretungen sowie von Kündigungen, Änderungen und Widerrufen der genannten Rechtsinstitute. Da in diesem Bereich sensible Daten der betroffenen Personen verarbeitet werden, bedarf es spezieller Rechtsschutzvorkehrungen, die in § 140h NO sowie den auf der Grundlage des § 140a Abs. 2 Z 8 NO ergangenen Richtlinien der Österreichischen Notariatskammer vom 4.6.2007 für das Österreichische Zentrale Vertretungsverzeichnis (ÖZVV-RL 2007), daneben aber auch in den anzuwendenden Verfahrensvorschriften insbesondere des AußStrG getroffen sind. Die angesprochenen Regelungen dienen ferner dem Schutz des Geschäftsverkehrs und damit – entsprechend der Öffnungsklausel des Art. 23 Abs. 1 lit. i DSGVO – der Sicherstellung der Rechte und Freiheiten anderer Personen.

Das von der Österreichischen Notariatskammer schon bald nach dem Inkrafttreten des Patientenverfügungs-Gesetzes eingerichtete „Patientenverfügungsregister des österreichischen Notariats“ dient – wie im neuen § 140i NO ausdrücklich klargestellt – der Registrierung von vor einem Notar errichteten oder sonst wirksam zustande gekommenen Patientenverfügungen. Die Registrierung, die nur auf Verlangen der Partei vorzunehmen ist, soll die Auffindbarkeit von Patientenverfügungen erleichtern und liegt damit im ausschließlichen Interesse des Verfügenden. Rechte Dritter sind hier nicht berührt, diesen können daher auch keine Rechte nach Art. 12 bis 22 und 34 DSGVO zukommen. Anfragen zu im Patientenverfügungsregister des österreichischen Notariats registrierten Patientenverfügungen können durch zu einer medizinischen Behandlung befugte Personen oder Einrichtungen im Weg des Österreichischen Roten Kreuzes gestellt werden. Die Patientenverfügung selbst wird im Patientenverfügungsregister des österreichischen Notariats nicht gespeichert. Liegt eine entsprechende Anordnung des Verfügenden vor, so kann die Patientenverfügung aber auch direkt dem abfragenden Arzt oder der abfragenden Krankenanstalt zur Verfügung gestellt werden.

Einer Partei ist über ihr Ersuchen im Weg eines Notars Einsicht in das Patientenverfügungsregister des österreichischen Notariats hinsichtlich aller ihre Person betreffenden aufrechten Registrierungen zu gewähren. Der Notar hat diesfalls anhand der Daten der Partei eine entsprechende Abfrage bei der Österreichischen Notariatskammer zu veranlassen. Über das – gegebenenfalls auch negative – Ergebnis der Suche ist der Partei ein entsprechender Registerausdruck zur Verfügung zu stellen.

Ausdrücklich hingewiesen sei in diesem Zusammenhang noch darauf, dass die verlässliche Auffindbarkeit und Verfügbarkeit von Patientenverfügungen einen wichtigen Punkt im Rahmen der laufenden Arbeiten des Bundesministeriums für Arbeit, Soziales, Gesundheit und Konsumentenschutz an der Weiterentwicklung der Elektronischen Gesundheitsakte (ELGA) darstellt. Die Ergebnisse dieser Arbeiten werden demgemäß auch ganz wesentlich für die künftige Bedeutung und Rolle (wie auch überhaupt für den weiteren Bestand) der Patientenverfügungsregister des österreichischen Notariats und der österreichischen Rechtsanwälte sein.

Angesichts des dargestellten umfangreichen und spezifisch abgestimmten Schutzregimes im Bereich der genannten Register, Archive und Verzeichnisse ist bei diesen jeweils die vorgeschlagene, auf Art. 23 Abs. 1 lit. i und j DSGVO beruhende datenschutzrechtliche Sonderregelung gerechtfertigt. Konkret wird vorgesehen, dass sich bei den in diesen Bereichen vorzunehmenden Datenverarbeitungen die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie die sich aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten des Einzelnen sowie deren Durchsetzung nach den Vorschriften dieses Bundesgesetzes und der nach § 140a Abs. 2 Z 8 erlassenen Richtlinien, im Fall des Urkundenarchivs ferner nach den Vorschriften des § 91c GOG richten.

Daneben bleibt die Zuständigkeit der Datenschutzbehörde als Aufsichtsbehörde unberührt. Ihre Zuständigkeit reicht dabei aber nur so weit, als Rechte und Pflichten des Einzelnen nach der DSGVO bestehen.

Für die sonstigen Rechte und Pflichten des Verantwortlichen nach der DSGVO soll mit der vorgeschlagenen Bestimmung überdies eine Verteilung der Aufgaben der jeweiligen Verantwortlichen im Sinn des Art. 4 Z 7 zweiter Satzteil DSGVO vorgenommen werden. Bei diesen sonstigen Rechten und Pflichten des Verantwortlichen handelt es sich etwa um die Verantwortung für Techniksicherheit (technische und organisatorische Datenschutzvorkehrungen – Art. 24, 25 DSGVO), die Zusammenarbeit mit Auftragsverarbeitern (Art. 28 DSGVO), die Zusammenarbeit mit der Datenschutzbehörde (Art. 31 DSGVO) und die Datensicherheit (Art. 32 ff DSGVO). Für diese sollen die Rechte und Pflichten des Verantwortlichen für die Datenverarbeitungen (soweit die diesbezüglichen Bestimmungen der DSGVO im Zusammenhang mit den jeweiligen Datenanwendungen des Notariats anwendbar sind) die Österreichische Notariatskammer treffen, wenn nicht in der Notariatsordnung, (gegebenenfalls) in § 91c GOG oder in den nach § 140a Abs. 2 Z 8 NO erlassenen Richtlinien eine Zuständigkeit des einzelnen Notars angeordnet ist.

Zu Z 14 (§ 168 NO):

Das zu § 20 Abs. 4 und 5 DSt Gesagte gilt sinngemäß.

Zu Art. 109 (Änderung der Rechtsanwaltsordnung)

Zu Z 1 (§ 9 Abs. 3a RAO):

Das Gebot der anwaltlichen Verschwiegenheit zählt zu den tragenden Säulen des Anwaltsberufs. Das Recht auf – und damit verbunden – die Pflicht des Rechtsanwalts zur Verschwiegenheit ist unverzichtbares Kernelement der Rechtsstaatlichkeit und unerlässlich für den Zugang zum Recht und das Grundrecht auf ein faires Verfahren (*Manhart*, Verschwiegenheit und Doppelvertretung, AnwBl 2014, 161 mwN). Eine Anwaltschaft ohne streng verstandene Verschwiegenheitsverpflichtung ist nicht denkbar. Für die berufsmäßige Parteienvertretung durch Rechtsanwälte kommt dem Umstand besondere Bedeutung zu, dass sich Klienten darauf verlassen können, dass von Seiten des Rechtsanwaltes und seiner Mitarbeiter keinerlei Informationen an Dritte gelangen. Erst dieses Vertrauen ermöglicht die Offenheit des Klienten gegenüber seinem Rechtsanwalt, die erforderlich ist, damit seine Interessen bestmöglich gewahrt werden können.

Schutzobjekt der anwaltlichen Verschwiegenheitspflicht sind die Parteiinteressen. Jedermann, der sich in seinen Angelegenheiten an einen berufsmäßigen Parteienvertreter wendet, muss darauf vertrauen können, dass er nicht gerade durch Betrauung eines Parteienvertreters und Informationserteilung an diesen Beweismittel gegen sich schafft. Fehlt dieser Schutz, so fehlt ein wesentliches Element des Rechts, sich in seinen Angelegenheiten eines Rechtsbeistands zu bedienen (VfSlg. 10.291/1984; RIS-Justiz RS0116762; *Lehner* in *Engelhart/Hoffmann/Lehner/Rohregger/Vitek*, RAO[9] § 9 RAO Rz 24).

§ 9 Abs. 3 RAO stellt damit im Zusammenhang bereits bisher klar, dass dieses Recht des Rechtsanwalts auf Verschwiegenheit nicht (durch gerichtliche oder sonstige behördliche Maßnahmen) umgangen werden darf. In gleicher Weise dürfen aber auch die durch die DSGVO eingeräumten Rechte nicht dazu führen, dass es zu einer entsprechenden Umgehung kommt. Eben dies wird durch Art. 23 Abs. 1 lit. i und j DSGVO sichergestellt, der Beschränkungen der Rechte der betroffenen Personen im Sinn der Art. 12 ff DSGVO durch Rechtsvorschriften der Mitgliedstaaten dann zulässt, wenn diese Maßnahmen „den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“ oder „die Durchsetzung zivilrechtlicher Ansprüche“ sicherstellen.

Auf dieser Grundlage und diesen Überlegungen beruht der neu vorgeschlagene § 9 Abs. 3a RAO, der vorsieht, dass die Rechte der betroffenen Person (im Verständnis des Art. 4 Z 1 DSGVO) nur dann und lediglich insoweit zur Anwendung kommen, als dem nicht das Recht des Rechtsanwalts auf Verschwiegenheit zum Schutz der Partei oder der Rechte und Freiheiten anderer Personen oder der Durchsetzung zivilrechtlicher Ansprüche entgegensteht. Dies ist deshalb notwendig, weil andernfalls die Gefahr bestünde, dass etwa der (Prozess-)Gegner einer zivilrechtlichen Streitigkeit im Weg des Informations- und Auskunftsrechts nach der DSGVO Auskünfte aus den Unterlagen und Akten des gegnerischen Rechtsanwalts erhalten könnte, was den Interessen der von diesem vertretenen Partei diametral entgegenstehen würde. Angesichts der Mannigfaltigkeit der hier möglichen Konstellationen ist gleichzeitig auch klar, dass eine generelle Beurteilung (und Anordnung) im Vorhinein, ob und inwieweit diese Beschränkung zum Tragen kommt, nicht möglich ist; dies ist gegebenenfalls vielmehr jeweils anhand der konkreten Umstände des Einzelfalls zu prüfen und zu bewerten.

Die Beschränkung der Betroffenenrechte geht (nur) so weit, wie dies das Recht des Rechtsanwalts auf Verschwiegenheit zur Sicherstellung des Schutzes der Partei oder der Rechte und Freiheiten anderer Personen oder der Durchsetzung zivilrechtlicher Ansprüche erfordert, ist also lediglich punktuell und erfolgt unter klar definierten Voraussetzungen. Allfällige Kontrollbefugnisse der Datenschutzbehörde als Aufsichtsbehörde bleiben unberührt.

Zu Z 2, 5, 6 und 8 (§§ 10a Abs. 8, 36 Abs. 1 Z 6, 8 und 9 sowie Abs. 1a und 37 Abs. 1 Z 7 RAO):

Das zu § 140b Abs. 7 NO Gesagte gilt für die Führung der Treuhandeinrichtungen durch die Rechtsanwaltskammern sinngemäß.

Die Führung der Treuhandeinrichtungen ist im Bereich der Rechtsanwaltschaft insbesondere durch § 10a RAO sowie die nach § 27 Abs. 1 lit. g RAO von den Rechtsanwaltskammern für ihren jeweiligen Bereich erlassenen Richtlinien geregelt. Nach diesen Bestimmungen sollen sich nach dem Vorschlag daher auch die aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung richten. Daneben bleibt die Zuständigkeit der Datenschutzbehörde als Aufsichtsbehörde unberührt. Ihre Zuständigkeit reicht dabei aber nur so weit, als Rechte und Pflichten des Einzelnen nach der DSGVO bestehen.

Sonstige Rechte und Pflichten des Verantwortlichen für diese Datenverarbeitungen treffen die Rechtsanwaltskammer, soweit nicht in diesem Bundesgesetz oder in den nach § 27 Abs. 1 lit. g RAO erlassenen Richtlinien eine Zuständigkeit des einzelnen Rechtsanwalts angeordnet ist.

Eine entsprechende Ausgangssituation besteht auch bei dem vom Österreichischen Rechtsanwaltskammertag eingerichteten und geführten anwaltlichen Urkundenarchiv sowie bei zwei vom Österreichischen Rechtsanwaltskammertag im Rahmen der anwaltlichen Selbstverwaltung geführten Registern, nämlich dem Patientenverfügungsregister der österreichischen Rechtsanwälte und dem Testamentsregister der österreichischen Rechtsanwälte. Die insofern erforderlichen datenschutzrechtlichen Anpassungen sollen dabei zugleich zum Anlass genommen werden, die beiden genannten Register auf eine eindeutige gesetzliche Grundlage zu stellen.

Das anwaltliche Urkundenarchiv dient der Speicherung von öffentlichen und privaten Urkunden (§ 36 Abs. 1 Z 4 RAO) insbesondere zum Zweck des elektronischen Urkundenverkehrs mit den Gerichten (§ 91c GOG).

Mit der Speicherung im Urkundenarchiv sollen die Rechte der Parteien geschützt und (gegebenenfalls) die Durchsetzung ihrer zivilrechtlichen Ansprüche sichergestellt werden. Die datenschutzrechtliche Sphäre der Parteien ist durch die vom Österreichischen Rechtsanwaltskammertag nach § 37 Abs. 1 Z 7 RAO zu erlassenden Richtlinien sowie die anzuwendenden Verfahrensvorschriften abgesichert. In den Richtlinien sind dabei neben den Modalitäten des elektronischen Zugangs und der Einsichtnahme einschließlich der Erteilung und der zeitlichen Ausgestaltung der Einsichtsberechtigungen der Parteien und der von diesen ermächtigten Personen auch die Protokollierung in Ansehung der Speichervorgänge und die zu erteilenden Auskünfte zu regeln.

Zum Patientenverfügungsregister der österreichischen Rechtsanwälte darf zunächst auf die Ausführungen zum neu vorgeschlagenen § 140i NO verwiesen werden. Ebenso wie das entsprechende Register des Notariats hat auch das Patientenverfügungsregister der österreichischen Rechtsanwälte den (alleinigen) Zweck, das Auffinden von Patientenverfügungen sicherzustellen bzw. zu erleichtern. Eine Registrierung und die daraus resultierende Datenverfügbarkeit dient damit ausschließlich Interessen des Verfügenden, ohne dass Rechte Dritter beeinflusst werden könnten. Voraussetzung für eine Registrierung ist ein entsprechendes Ersuchen der Partei, die dabei auch verlangen kann, dass gleichzeitig eine Speicherung der Patientenverfügung (ihres elektronischen Abbildes) erfolgt. Der Zugang zu den gespeicherten Daten und einer gegebenenfalls gespeicherten Patientenverfügung ist den zu einer medizinischen Behandlung befugten Personen oder Einrichtungen zu ermöglichen. Zur Regelung der näheren Voraussetzungen für die Registrierung und die allfällige Speicherung solcher Patientenverfügungen auf Verlangen der Partei sowie den Zugang zu und die Löschung von registrierten Daten einschließlich der Festlegung der zur Deckung des damit verbundenen Aufwands notwendigen Gebühren sieht der vorgeschlagene § 37 Abs. 1 Z 7 RAO eine Richtlinienermächtigung an den Österreichischen Rechtsanwaltskammertag vor.

Wie beim Patientenverfügungsregister des österreichischen Notariats sei auch an dieser Stelle nochmals ausdrücklich darauf hingewiesen, dass die verlässliche Auffindbarkeit und Verfügbarkeit von Patientenverfügungen einen wichtigen Punkt im Rahmen der laufenden Arbeiten des Bundesministeriums für Arbeit, Soziales, Gesundheit und Konsumentenschutz an der Weiterentwicklung der Elektronischen Gesundheitsakte (ELGA) darstellt. Die Ergebnisse dieser Arbeiten werden demgemäß auch ganz wesentlich für die künftige Bedeutung und die Rolle (wie auch überhaupt für den weiteren Bestand) der Patientenverfügungsregister des österreichischen Notariats und der österreichischen Rechtsanwälte sein.

Im Testamentsregister der österreichischen Rechtsanwälte können auf Verlangen einer Partei letztwillige Verfügungen und deren Verwahrungsort durch einen Rechtsanwalt registriert werden. Im Testamentsregister elektronisch erfasst werden dabei nicht das Testament selbst, sondern jene Daten, die ein verlässliches Auffinden des Testaments gewährleisten sollen. Eine Registrierung liegt damit bis zum Wirksamwerden des Testaments im ausschließlichen Interesse des Testators. Nach dessen Ableben ist der Gerichtskommissär im anschließenden Verlassenschaftsverfahren gemäß § 145a Abs. 2 AußStrG verhalten, neben dem Österreichischen Zentralen Testamentsregister auch das Testamentsregister der österreichischen Rechtsanwälte abzufragen und das Ergebnis zu dokumentieren. Ein solcherart (gegebenenfalls) hervorgekommenes Testament ist in der Folge nach den dann anzuwendenden Verfahrensvorschriften gerichtlich abzuhandeln.

Auch beim anwaltlichen Urkundenarchiv sowie beim Patientenverfügungs- und Testamentsregister der österreichischen Rechtsanwälte erscheint es angesichts der bei diesen zur Anwendung kommenden umfangreichen und spezifisch abgestimmten Schutzregime gerechtfertigt, eine auf Art. 23 Abs. 1 lit. i und j DSGVO beruhende datenschutzrechtliche Sonderregelung vorzusehen. Nach dieser sollen sich bei den in diesen Bereichen vorzunehmenden Datenverarbeitungen die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie die sich aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten des Einzelnen sowie deren

Durchsetzung nach den Vorschriften dieses Bundesgesetzes und der nach § 37 Abs. 1 Z 7 erlassenen Richtlinien, im Fall des anwaltlichen Urkundenarchivs ferner nach den Vorschriften des § 91c GOG richten.

Daneben bleibt die Zuständigkeit der Datenschutzbehörde als Aufsichtsbehörde unberührt. Ihre Zuständigkeit reicht dabei aber nur so weit, als Rechte und Pflichten des Einzelnen nach der DSGVO bestehen.

Für die sonstigen Rechte und Pflichten des Verantwortlichen nach der DSGVO soll mit der vorgeschlagenen Bestimmung überdies eine Verteilung der Aufgaben der jeweiligen Verantwortlichen im Sinn des Art. 4 Z 7 zweiter Satzteil DSGVO vorgenommen werden. Bei diesen sonstigen Rechten und Pflichten des Verantwortlichen handelt es sich etwa um die Verantwortung für Techniksicherheit (technische und organisatorische Datenschutzvorkehrungen – Art. 24, 25 DSGVO), die Zusammenarbeit mit Auftragsverarbeitern (Art. 28 DSGVO), die Zusammenarbeit mit der Datenschutzbehörde (Art. 31 DSGVO) und die Datensicherheit (Art. 32 ff DSGVO). Für diese sollen die Rechte und Pflichten des Verantwortlichen für die Datenverarbeitungen (soweit die diesbezüglichen Bestimmungen der DSGVO im Zusammenhang mit den jeweiligen Datenanwendungen der Rechtsanwaltschaft anwendbar sind) den Österreichischen Rechtsanwaltskammertag treffen, wenn nicht in der Rechtsanwaltsordnung, (gegebenenfalls) in § 91c GOG oder in den nach § 37 Abs. 1 Z 7 RAO erlassenen Richtlinien eine Zuständigkeit des einzelnen Rechtsanwalts angeordnet ist.

Zu Z 3, 5 und 7 (§§ 23 Abs. 2a, 36 Abs. 1 Z 7 und 36 Abs. 6 RAO):

Das zu §§ 134 Abs. 4 und 140a Abs. 3a NO Gesagte gilt sinngemäß. Angesichts der von den Rechtsanwaltskammern einzurichtenden und aufrecht zu erhaltenden Einrichtungen zur Versorgung ihrer Mitglieder und deren Angehörigen ist die Ermächtigung zur Verarbeitung personenbezogener Daten sowohl im Bereich der Rechtsanwaltskammern als auch im Bereich des Österreichischen Rechtsanwaltskammertags ausdrücklich auch auf solche Daten allfälliger Anspruchsberechtigter oder Begünstigter aus den Versorgungseinrichtungen der Rechtsanwaltskammern zu beziehen.

Zu berücksichtigen ist ferner, dass die Rechtsanwälte und Rechtsanwaltsanwärter zwar jeweils Mitglieder „ihrer“ Rechtsanwaltskammer, nicht aber auch Mitglieder des Österreichischen Rechtsanwaltskammertags sind. Angesichts dessen erscheint es aufgrund der dem Österreichischen Rechtsanwaltskammertag auch in Bezug auf die einzelnen Standesmitglieder gesetzlich zukommenden bzw. durch die Rechtsanwaltskammern gemäß § 36 Abs. 3 RAO übertragenen Aufgaben geboten, die Erhebung personenbezogener Daten der Mitglieder der Rechtsanwaltskammern und allfälliger Anspruchsberechtigter oder Begünstigter aus den Versorgungseinrichtungen der Rechtsanwaltskammern sowie die Erfassung und Bereitstellung dieser Daten in einer Datenbank und deren Verwendung für die Zwecke der Versorgungseinrichtungen der Rechtsanwaltskammern ausdrücklich als Aufgabe des Österreichischen Rechtsanwaltskammertags zu definieren.

Bedacht zu nehmen ist in diesem Kontext ferner darauf, dass die Rechtsanwaltskammern wie auch der Österreichische Rechtsanwaltskammertag im Rahmen ihres jeweiligen gesetzlichen Zuständigkeitsbereichs gegebenenfalls auch Daten von Personen zu verarbeiten haben, die (noch) nicht Standesangehörige sind (ein Beispiel dafür ist etwa die begehrte Eintragung in die Liste der Rechtsanwaltsanwärter).

Zu Z 4 (§ 36 Abs. 1 Z 5 RAO):

Mit dem neu formulierten § 36 Abs. 1 Z 5 RAO sollen die dem Österreichischen Rechtsanwaltskammertag nach dieser Bestimmung bereits jetzt implizit zukommende Befugnis zur Bereitstellung eines elektronischen Verzeichnisses der in die Listen der österreichischen Rechtsanwaltskammern eingetragenen Rechtsanwälte ausdrücklich geregelt und die Bereitstellung des „elektronischen Rechtsanwaltsverzeichnisses“ als Aufgabe des Österreichischen Rechtsanwaltskammertags festgelegt werden. Sowohl das elektronische Rechtsanwaltsverzeichnis als auch das elektronische Verzeichnis für die Anwaltssignaturen (das zulässigerweise gemeinsam mit dem elektronischen Rechtsanwaltsverzeichnis geführt werden kann) müssen über die Website des Österreichischen Rechtsanwaltskammertags allgemein zugänglich sein.

Zu Art. 110 (Änderung des StAG):

Zu Z 1 (§ 34a Abs. 2a StAG):

Siehe grundsätzlich die Erläuterungen zu Artikel 5 Z 2 (§ 85a GOG).

Da Staatsanwaltschaften aufgrund des Art. 90a B-VG als Organe der Gerichtsbarkeit anzusehen sind, kommt nach Auffassung des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz der in seiner geltenden Fassung auf eine Rechtsverletzung durch ein Organ der Gerichtsbarkeit

abstellende § 85 GOG auch im staatsanwaltschaftlichen Bereich zur Anwendung (vgl. in diesem Sinn auch *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 63 zur alten Rechtslage mit dem Hinweis auf Burgstaller in *Korinek/Holoubek* [Hrsg], Österreichisches Bundesverfassungsrecht Art 90a B-VG Rz 21 und DSK vom 8.5.2009, K121.472/0003-DSK/2009/00 und vom 18.11.2009, K121.561/0004-DSK/2009, wonach Akte der aufgrund von Art. 90a B-VG als Organe der Gerichtsbarkeit anzusehenden Staatsanwaltschaften der Entscheidungsgewalt der DSK entzogen sind). Um den Anwendungsbereich der Bestimmung infolge deren vorgeschlagener Neufassung nicht einzuschränken, soll deren Regelungsgehalt nunmehr auch ausdrücklich in den – schon derzeit umfassten – staatsanwaltschaftlichen Bereich überführt werden.

Zu Z 2 (§ 34a Abs. 6 StAG):

Nach § 36 Abs. 2 Z 8 DSG idF BGBl. I. Nr. 120/2017 ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff ersetzt jenen des Auftraggebers nach § 4 Abs. 4 DSG 2000. Der Verantwortliche zeichnet für die Einhaltung der durch §§ 74 f StPO bzw. § 37 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 festgelegten Kriterien der Zulässigkeit einer Datenverarbeitung verantwortlich, ihn treffen unter Berücksichtigung der durch die StPO (des DSG) normierten Voraussetzungen die Pflichten zur Information, Auskunftserteilung, Berichtigung und Löschung personenbezogener Daten und Einschränkung deren Verarbeitung.

Nach Art. 3 Z 8 DS-RL gilt, dass für den Fall, dass die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind, der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden können. Die Staatsanwaltschaften und Oberstaatsanwaltschaften sowie die Generalprokuratur dürfen die für die Ausübung ihrer Aufgaben erforderlichen personenbezogenen Daten nach den Vorgaben der Verfahrensgesetze, welche Zweck und Mittel der jeweils rechtmäßigen Datenverarbeitung im Strafverfahren bestimmen, verarbeiten. Ergänzend dazu legen die maßgeblichen Rechtsvorschriften etwa zur Akten- und Registerführung und zu den hiefür bereitgestellten technischen Applikationen (derzeit die Verfahrensautomation Justiz [VJ]) die zulässigen Mittel der Verarbeitung fest.

Aufgrund des Umstands, dass die Struktur der seitens der jeweils verfahrensführenden Staatsanwaltschaft, der Oberstaatsanwaltschaft oder der Generalprokuratur verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellte Applikation Verfahrensautomation Justiz (VJ) vorgegeben wird, sollen die jeweils fallbearbeitende Staatsanwaltschaft, die Oberstaatsanwaltschaft oder die Generalprokuratur und das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz die Position des Verantwortlichen wahrnehmen. Die Wahrnehmung der Rechte und Pflichten des Verantwortlichen nach der StPO (aufgrund des Verweises in § 74 Abs. 1 StPO subsidiär des DSG) soll dabei ausschließlich die jeweils verfahrensführende Staatsanwaltschaft, die Oberstaatsanwaltschaft oder die Generalprokuratur treffen.

Eine der Bestimmung des § 89q Abs. 2 GOG vergleichbare Regelung soll es für den staatsanwaltschaftlichen Bereich hingegen nicht geben: Eine Auflösung des Spannungsverhältnisses zwischen dem Recht des Beschuldigten auf Information über das gegen ihn geführte Strafverfahren sowie seine wesentlichen Rechte einerseits und dem legitimen Geheimhaltungsinteresse der Staatsanwaltschaft bei Befürchtung, dass durch eine entsprechende Information ansonsten der Zweck der Ermittlungen gefährdet wäre, ist nur im Einzelfall durch eine den Geboten der Gesetz- und Verhältnismäßigkeit gemäß § 5 StPO Rechnung tragende Anwendung von § 50 Abs. 1 letzter Satz StPO auflösbar. Aus dem Wortlaut des § 50 Abs. 1 StPO („Information…darf nur so lange unterbleiben, als besondere Umstände befürchten lassen…“) ergibt sich, dass der Aufschub der Information des Beschuldigten restriktiv zu handhaben ist (*Achammer*, in *Fuchs/Ratz*, WK StPO § 50 Rz 5f). Jedenfalls ist der Beschuldigte vor bzw. unmittelbar nach der Ausübung von Zwang oder vor seiner Vernehmung zur Sache über den gegen ihn bestehenden Tatverdacht und seine Rechte aufzuklären (EBRV 25 BlgNR 22. GP 68f; *Pilnacek/Pleischl,* Das neue Vorverfahren, Rz 185; *Fabrizy*, StPO[13] § 50 Rz 2). Darüber hinaus unterliegt der Aufschub der Information des Beschuldigten im Wege des Einspruchs wegen Rechtsverletzung gemäß § 106 StPO der Kontrolle durch die unabhängigen Gerichte. Das durch den grundsätzlichen Zweck des Ermittlungsverfahrens bedingte Hindernis für eine aktive Verständigung des Beschuldigten darf nicht dadurch umgangen werden, dass dieser aktiv eine entsprechende Anfrage an eine oder mehrere nicht verfahrensführende Staatsanwaltschaften oder auch das Bundesministerium für Justiz richtet, weil schon mit einer Beantwortung einer solchen Anfrage dahin, „dass die Auskunft nicht erteilt werde“ bzw. „der begehrten Auskunft die Bestimmung des § 50 Abs. 1 dritter Satz StPO entgegen stehe“, der Zweck der Norm (nämlich die Geheimhaltung) vereitelt würde. Dasselbe gilt für einen Hinweis, an welche konkrete, nämlich verfahrensführende, Staatsanwaltschaft sich ein Auskunftswerber wenden solle. Im Ergebnis ist auch zur Vermeidung einer uneinheitlichen Praxis die begehrte Auskunft über die bei einer

Staatsanwaltschaft gespeicherten personenbezogenen Daten oder dort anhängige Ermittlungsverfahren nur von der jeweils verfahrensführenden Staatsanwaltschaft zu erteilen, weil nur diese allein zur hinreichenden Beurteilung in der Lage ist, ob über solche Daten bzw. ein dort anhängiges Ermittlungsverfahren Auskunft erteilt werden kann.

Zu Z 3 (§ 42 Abs. 20 StAG):

Die Bestimmung regelt das Inkrafttreten.

Zu Art. 111 (Änderung der StPO):

Zu Z 1, 4 und 5 (Eintrag zu § 74 im Inhaltsverzeichnis, Überschrift von § 74 und § 74 Abs. 1 StPO):

Gerichte, Staatsanwaltschaften, Finanzstrafbehörden, Sicherheitsbehörden und sonstige staatliche Behörden, die mit der Erfüllung von Aufgaben im Strafverfolgungsbereich zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit betraut sind, fallen im Rahmen ihrer Aufgabenerfüllung in den Anwendungsbereich der DS-RL.

Deren Umsetzung erfolgte mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017. In dessen 3. Hauptstück finden sich explizite Regelungen zur Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung (§§ 36ff).

Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausdrücklich klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. So sind etwa insbesondere die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten leges speciales zum 3. Hauptstück des DSG. Ebenso sind die Bestimmungen über die Aufgaben der Datenschutzbehörde nach § 32 DSG – zumindest in den Fällen der Z 4, 5 und 8 – im Bereich des Strafverfahrens nicht anwendbar, an deren Stelle stehen die entsprechenden Rechtsbehelfe der StPO (bzw. subsidiär des GOG), die gerichtlichen Rechtsschutz gewährleisten, zur Verfügung. Einer ausdrücklichen gesetzlichen Anordnung des im Bericht des Verfassungsausschusses dargelegten Vorrangs des strafprozessualen Rechtsschutzsystems gegenüber der Aufsicht durch die Datenschutzbehörde bedarf es nicht: Gemäß § 31 Abs. 1 erster Satz DSG wird die Datenschutzbehörde als nationale Aufsichtsbehörde für den in § 36 Abs. 1 DSG genannten Anwendungsbereich eingerichtet. Nach dieser Bestimmung ist die Datenschutzbehörde jedoch für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig. Diese Ausnahme beruht auf der verpflichtenden Vorgabe des Art. 45 Abs. 2 DS-RL, wodurch sichergestellt werden soll, dass die Unabhängigkeit der Gerichte im Rahmen ihrer rechtsprechenden Tätigkeit gewahrt bleibt, obwohl die Richtlinie selbst auch für die Tätigkeit der Gerichte gilt (vgl. EG 80 der DS-RL). Aufgrund der Ausnahme in § 31 Abs. 1 zweiter Satz DSG ist ein doppelter Rechtsschutz von vornherein ausgeschlossen, weil in diesem Bereich ausschließlich die Bestimmungen der Materiengesetze (StPO, GOG, StAG) zur Anwendung gelangen. Im Ergebnis gilt daher der bereits in der geltenden Fassung des § 74 Abs. 1 StPO zum Ausdruck kommende Grundsatz der lediglich subsidiären Geltung des DSG gegenüber der StPO (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 2 f; 63) auch weiterhin. Durch den Entfall der Wortfolge „im Einzelnen“ wird zum Ausdruck gebracht, dass der Vorrang der StPO „generalisierend“ wirkt und sich nicht nur auf jene Konstellationen bezieht, in denen explizite Bestimmungen in der StPO bestehen, die den auf exakt denselben Regelungsgehalt abzielenden Bestimmungen des DSG voranstehen. Die Informations- und Auskunftspflichten bleiben ausschließlich in den in der StPO angeführten Fällen bestehen.

Entsprechend § 38 DSG ist die Verarbeitung personenbezogener Daten, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, wenn sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird. Es soll daher in Ergänzung der bestehenden Verpflichtung zur Beachtung des Grundsatzes der Gesetz- und Verhältnismäßigkeit in § 74 Abs. 2 StPO eine ausdrückliche gesetzliche Grundlage für die Zulässigkeit der Datenverarbeitung durch Kriminalpolizei, Staatsanwaltschaften und (Straf-)Gerichte in § 74 Abs. 1 StPO geschaffen werden. Die von diesen wahrzunehmenden Aufgaben werden im Wesentlichen durch § 1 Abs. 1 StPO bestimmt: Kriminalpolizei, Staatsanwaltschaften und Gerichte haben Straftaten aufzuklären, verdächtige Personen zu verfolgen und damit zusammenhängende Entscheidungen zu treffen. Ebenso erfasst ist die Tätigkeit der im Ermittlungs- oder Hauptverfahren durch die Staatsanwaltschaft oder das Gericht bestellten Sachverständigen und Dolmetscher. Die offene

Formulierung berücksichtigt weiters, dass die Staatsanwaltschaft nicht nur im Ermittlungsverfahren als dessen Leiterin, sondern in weiterer Folge auch im Hauptverfahren als Beteiligte (§ 210 Abs. 2 StPO) tätig wird und ermöglicht ihr so auch in diesem Verfahrensstadium die Verarbeitung entsprechender personenbezogener Daten; gleiches gilt für die Tätigkeiten der Oberstaatsanwaltschaft in den Strafverfahren vor dem Oberlandesgericht (§ 21 Abs. 1 StPO) und der Generalprokuratur in den Strafverfahren vor dem Obersten Gerichtshof (§ 22 StPO). Für die Strafgerichte ist auf die ebenfalls vorgeschlagene Bestimmung des § 85a GOG zu verweisen, in der zur Konkretisierung der in § 74 Abs. 1 StPO vorgeschlagenen Formulierung auf die Angelegenheiten der Strafgerichtsbarkeit abgestellt wird. Diesem Begriff liegt ein weites Verständnis zugrunde, wodurch die Verarbeitung personenbezogener Daten nicht nur im Bereich der gerichtlichen Entscheidungstätigkeit, sondern auch in jenem der zur unabhängigen Rechtsprechung zählenden kollegialen Justizverwaltung (Art. 87 Abs. 2 B-VG) unter den durch § 74 Abs. 2 StPO normierten Prämissen zulässig ist. § 74 Abs. 1 StPO schafft auch eine Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten, weil die hiefür in § 39 DSG normierten Voraussetzungen sowohl in § 74 Abs. 1 als auch in Abs. 2 StPO Deckung finden.

Soweit Kriminalpolizei, Staatsanwaltschaften und Gerichte auch mit der Erfüllung anderweitiger Aufgaben betraut sind, unterliegen sie in Bezug auf diese Tätigkeiten nicht den Vorschriften des 3. Hauptstücks des DSG, sondern der DSGVO (zur Abgrenzung von Grenzfällen siehe den Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 17 f).

Die vorgeschlagene Änderung der Überschrift des § 74 StPO bezweckt eine Anpassung an die Terminologie des DSG idF BGBl. I. Nr. 120/2017.

Zu Z 3 (§ 54, § 76 Abs. 4 StPO):

Die vorgeschlagenen Änderungen betreffen Anpassungen von Verweisen an das DSG, inhaltliche Änderungen sind damit nicht verbunden. Durch die Änderung des DSG mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I. Nr. 120/2017, leitet sich der Begriff der „schutzwürdigen Geheimhaltungsinteressen“ nunmehr ausschließlich aus der unverändert gebliebenen Verfassungsbestimmung des § 1 Abs. 1 DSG ab.

Zu Z 2, 6, 7, 9 bis 11 und 13 bis 18 (Eintrag zu § 75 im Inhaltsverzeichnis, § 74 Abs. 2, Überschrift von § 75, § 75 Abs. 3 und 4, § 76 Abs. 4, § 117 Z 1, § 141 Abs. 1 und 4, § 142 Abs. 2 und § 143 Abs. 1 und 2 StPO):

Die vorgeschlagenen Änderungen der StPO stellen redaktionelle und terminologische Anpassungen an die neue Struktur und Terminologie des DSG idF BGBl. I Nr. 120/2017 dar.

Zu Z 8 (§ 75 Abs. 1 StPO):

Die vorgeschlagenen Änderungen betreffen in erster Linie Anpassungen an die Terminologie des DSG idF BGBl. I. Nr. 120/2017.

Das Recht auf Berichtigung bzw. Vervollständigung personenbezogener Daten ist im Strafverfolgungskontext nur eingeschränkt durchsetzbar. Insbesondere sind davon keine nachträglichen Veränderungen von Aussagen bei Vernehmungen umfasst; hier bezieht sich die Richtigkeit und Vollständigkeit der personenbezogenen Daten auf die Übereinstimmung mit der Aussage selbst und nicht auf deren Inhalt (vgl. auch EG 47 der DS-RL bzw. den Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 23).

Während § 27 Abs. 1 DSG 2000 für die Berichtigung oder Löschung von Daten sowohl ein Antragsrecht (Z 1) als auch ein Vorgehen des Auftraggebers von Amts wegen (Z 2) vorsieht, findet sich in § 75 Abs. 1 StPO bislang keine entsprechende Regelung. Nach hA ist davon auszugehen, dass die Berichtigung entsprechend der Wertung des § 27 DSG 2000 sowohl von Amts wegen wie auch auf Antrag unverzüglich durchzuführen ist (*Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 75 Rz 1).

Zwar sieht § 45 Abs. 1 und 2 DSG idF BGBl. I. Nr. 120/2017 eine von § 27 Abs. 1 DSG 2000 abweichende Regelung dahingehend vor, dass ein Vorgehen von Amts wegen nur im Fall der Löschung von Daten, nicht jedoch bei einer bloßen Berichtigung möglich ist. Gleichwohl ergibt sich eine solche Verpflichtung aus § 37 Abs. 1 Z 4 iVm § 37 Abs. 3 DSG, weshalb dem jeweils verfahrensführenden Gericht oder der jeweils verfahrensführenden Staatsanwaltschaft als Verantwortlichem (siehe hierzu die vorgeschlagenen § 89q Abs. 2 GOG und § 34a Abs. 6 StAG) die Verpflichtung zur Löschung und Berichtigung von Daten von Amts wegen zukommen. Zur Verdeutlichung der sich aus verschiedenen Fundstellen des DSG schließenden Verpflichtungen wird vorgeschlagen, diese ausdrücklich in § 75 Abs. 1 StPO zu normieren.

Entsprechend § 45 Abs. 5 und 6 DSG idF BGBl. I. Nr. 120/2017 sollen von einer Berichtigung oder Löschung jene Behörden und Gerichte, denen diese personenbezogenen Daten übermittelt wurden (§ 76

Abs. 4 StPO) sowie von einer Berichtigung überdies jene Behörden und öffentlichen Dienststellen des Bundes, der Länder und der Gemeinden sowie andere durch Gesetz eingerichtete Körperschaften und Anstalten des öffentlichen Rechts, von denen die personenbezogenen Daten stammen, zu verständigen sein.

Zu Z 12 (§ 77 Abs. 2 StPO):

Die vorgeschlagene Neufassung des § 77 Abs. 2 StPO versteht sich als zentrale Grundlage der Zulässigkeit der Übermittlung personenbezogener Daten eines Strafverfahrens zu wissenschaftlichen Zwecken. Grundvoraussetzung der Anwendung ist, dass die Daten im Anwendungsbereich der DS-RL (entsprechend § 36 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 somit zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung) ermittelt wurden.

Unter Berücksichtigung des § 40 Abs. 1 und 2 DSG idF BGBl. I. Nr. 120/2017, der grundsätzliche Vorgaben zur Zulässigkeit der Übermittlung solcher Daten zu wissenschaftlichen Zwecken innerhalb des Anwendungsbereichs der DS-RL (etwa zu Präventionszwecken) und eines – in der Praxis weit häufiger vorkommenden – Zwecks außerhalb davon regelt, soll zur umfassenden Wahrung der Datenschutzrechte betroffener Personen eine Übermittlung nur möglich sein, wenn eine Pseudonymisierung (§ 36 Abs. 2 Z 5 DSG idF BGBl. I. Nr. 120/2017 = „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“) personenbezogener Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist und überdies das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Geheimhaltungsinteresse der betroffenen Personen erheblich überwiegt. Wie auch bisher dürfen Daten ferner nur zum Zweck einer nicht personenbezogenen Auswertung für wissenschaftliche oder historische Forschungszwecke oder vergleichbare im öffentlichen Interesse liegende Untersuchungen (worunter auch Archivzwecke zu verstehen sind) übermittelt werden. Ungeachtet der den Empfänger der Daten im Regelfall treffenden Vorgaben der DSGVO ist von diesem auch weiterhin § 54 StPO zu beachten.

Aufgrund der künftig erforderlichen sorgfältigen Abwägung des vom Antragsteller hinreichend darzulegenden öffentlichen Interesses an der Forschungsarbeit einerseits und des schutzwürdigen Geheimhaltungsinteresses der betroffenen Personen andererseits soll den betroffenen Personen unter Berücksichtigung des Umstands, dass das öffentliche Interesse jenes auf Geheimhaltung erheblich zu überwiegen hat, die Auswertung ohnedies nur nicht personenbezogen erfolgen darf und der Empfänger als Verantwortlicher im Regelfall den umfassenden Verpflichtungen der Verordnung (EU) 2016/679 sowie überdies der Bestimmung des § 54 StPO unterliegt, das Recht auf Auskunft (§ 44 DSG idF BGBl. I. Nr. 120/2017) nicht zukommen. Damit im Einklang treffen den verantwortlichen Übermittelnden auch keine Informationspflichten (§ 43 DSG idF BGBl. I. Nr. 120/2017). Der Ausschluss der Rechte der betroffenen Personen auf Information (§ 43 DSG) und auf Auskunft (§ 45 DSG) gründet auf Art. 15 Abs. 1 lit. e bzw. Art. 16 Abs. 4 lit. e der DS-RL (Freiheit der Wissenschaft nach Art. 17 StGG). Die Rechte der betroffenen Personen auf Berichtigung oder Löschung nach § 75 Abs. 1 StPO bleiben unberührt, jedoch sind diese im Zusammenhang mit einem Vorgehen nach § 77 Abs. 2 StPO ohnedies ohne Relevanz.

Zu Z 19 (§ 514 Abs. 37):

Die Bestimmung regelt das Inkrafttreten.

Zu Art. 112 (Änderung des Strafregistergesetzes):

Zu Z 1 und 2 (§ 1 Abs. 2 und 3 StRegG):

In § 1 Abs. 2 StRegG soll die Klarstellung erfolgen, dass die Führung des Strafregisters von der Landespolizeidirektion Wien als Verantwortliche gemäß Art. 4 Z 7 iVm Art. 24 der Datenschutz-Grundverordnung erfolgt.

In den gesetzlichen Regelungen wird zwar sowohl der Zweck der Datenverarbeitung als auch das Mittel, nämlich eine bestimmte zentrale Anwendung (das Strafregister), festgelegt, obwohl die DSGVO den Verantwortlichen grundsätzlich dadurch gekennzeichnet sieht, als eben dieser Mittel und Zweck festlegt. Die vorliegende Regelung orientiert sich daher daran, dass nach Art. 4 Z 7 der Datenschutz-Grundverordnung, wenn Zweck und Mittel durch das Recht der Mitgliedstaaten vorgesehen werden, der Verantwortliche oder die Kriterien der Benennung des Verantwortlichen auch nach diesem Recht vorgenommen werden können. In gegenständlicher Regelung wird die zur Vollziehung der Materie

zuständige Behörde, also die Landespolizeidirektion Wien, als Verantwortliche bezeichnet, die die Entscheidung über die konkrete Datenverarbeitung trifft. Insoweit ist davon auszugehen, dass die Regelung mit dem Unionsrecht jedenfalls im Einklang steht.

Zudem ist beabsichtigt, – ohne eine materielle Änderung der Rechtslage herbeizuführen – im Sinne der Transparenz (vgl. Erwägungsgrund 39 zur Datenschutz-Grundverordnung) in § 1 Abs. 3 StRegG ausdrücklich festzulegen, dass der Bundesminister für Inneres die Funktion des Auftragsverarbeiters gemäß Art. 8 Z 8 iVm Art. 28 Abs. 1 der Datenschutz-Grundverordnung ausübt. Darüber hinaus soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h der Datenschutz-Grundverordnung wahrzunehmen, da andernfalls der Abschluss einer Vereinbarung über die Datenschutzpflichten erforderlich wäre (vgl. Art. 28 Abs. 3Datenschutz-Grundverordnung). Außerdem soll er wie bisher weitere Auftragsverarbeiter in Anspruch nehmen können.

Hinsichtlich der Funktion als Auftragsverarbeiter ist vor dem verfassungsrechtlichen Hintergrund, dass der Bundesminister für Inneres oberstes Organ ist, nicht zu übersehen, dass ein Spannungsverhältnis vermutet werden könnte, da es zum Wesen eines Auftragsverarbeiters gehört, dass er nur im Auftrag oder nur mit Genehmigung des Verantwortlichen tätig wird (Art. 28 der Datenschutz-Grundverordnung). Verfassungswidrig wäre es, wenn vorgesehen würde, dass der Bundesminister in dieser Rolle an Willensbildungen anderer Stellen, also etwa der nachgeordneten Landespolizeidirektion Wien als Verantwortliche gebunden sein würde. Die vorgeschlagene Regelung sieht Derartiges nicht vor. Vielmehr erfolgt die Beauftragung und Bindung ausschließlich durch das Gesetz selbst. Dabei werden dem Bundesminister für Inneres in erster Linie Aufgaben übertragen, wie sie typischerweise einem Auftragsverarbeiter gemäß Art. 28 der Datenschutz-Grundverordnung zukommen, die eben – wie dies dort auch als zulässig erachtet wird – nicht im Rahmen eines Vertrages übertragen werden, sondern durch ein Rechtsinstrument des Mitgliedstaates, hier ein Gesetz. Insoweit kommt ihm aber auch nicht die Rolle eines Verantwortlichen zu, da er in keiner Weise die Entscheidung über die Verarbeitung der Daten trifft. Diese Entscheidung kommt allein der Landespolizeidirektion Wien zu. Wie dies bereits in den Erläuterungen zum DSG 1978 ausgeführt wird, ändern daran auch nichts die im öffentlichen Bereich bestehenden Weisungen an nachgeordnete Organe, im Rahmen ihrer Eigenzuständigkeit Datenverarbeitungen einzusetzen; dabei handelt es sich nicht um solche Aufträge, wie sie sich im Verhältnis von Auftraggeber und Dienstleister oder in der Terminologie der Datenschutz-Grundverordnung von Verantwortlichem und Auftragsverarbeiter darstellen. Diese Weisungen bilden nämlich nicht den unmittelbaren Anlass für die Aufnahme der Datenverarbeitung, sie wird vielmehr erst durch entsprechende Akte des angewiesenen Organs bewirkt (vgl. ErläutRV 554 BlgNR 16. GP 13).

Damit wird durch die vorgesehene Einbindung des Bundesministers für Inneres weder in die Position als oberstes Organ, noch in den geltenden Weisungszusammenhang eingegriffen.

Zu Z 3 und 4 (§ 8 Abs. 1, 2 und 5 StRegG):

Das umfassende Recht auf Berichtigung, Löschung sowie Einschränkung der Verarbeitung personenbezogener Daten des Betroffenen ergibt sich aus der Datenschutz-Grundverordnung (vgl. Art. 16, 17 und 18). Gemäß Art. 23 ist es jedoch zulässig, diesbezügliche Pflichten und Rechte im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern zum einen eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und zum anderen in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Zudem muss die Beschränkung näher normierte wichtige Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates sicherstellen.

Da es sich bei den Strafregisterdaten um vor allem für Zwecke der Strafrechtspflege und inneren Sicherheit essentielle Daten handelt, ist eine Beschränkung der Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung aus Gründen der öffentlichen Sicherheit gemäß Art. 23 Abs. 1 lit. c der Datenschutz-Grundverordnung, des Schutzes sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses gemäß Art. 23 Abs. 1 lit. e der Datenschutz-Grundverordnung und des Schutzes der betroffenen Person gemäß Art. 23 Abs. 1 lit. i der Datenschutz-Grundverordnung unbedingt erforderlich. Demzufolge sollen die genannten Rechte nur in Form eines spezifischen Feststellungsverfahrens wahrgenommen werden können. Da die Pflichten gegenüber dem Betroffenen nach der Datenschutz-Grundverordnung den Verantwortlichen treffen, soll künftig der Antrag bei der Landespolizeidirektion Wien einzubringen sein, die hierüber zu entscheiden hat. In Anbetracht der Tatsache, dass auf Basis der internen Aufzeichnungen des Bundesministeriums für Inneres in den vergangenen Jahren lediglich im Durchschnitt acht Anträge pro Jahr gestellt wurden, ist diesbezüglich für die Landespolizeidirektion Wien auch mit keinem erheblichen Mehraufwand zu rechnen. Der Betroffene soll demnach bei der Landespolizeidirektion Wien unter anderem die Feststellung beantragen können,

dass die Aufnahme oder Nichtaufnahme einer Verurteilung oder einer sich darauf beziehenden Entschließung oder Entscheidung in das Strafregister zu Unrecht erfolgte. Das Rechtsschutzverfahren ermöglicht die Überprüfung der Zulässigkeit, Richtigkeit und Vollständigkeit einer Registereintragung durch die Landespolizeidirektion Wien. Das Verfahren dient jedoch nicht der Überprüfung eines Strafurteils oder einer darauf bezugnehmenden Gerichtsentscheidung (vgl. *Kert* in *Fuchs/Ratz*, WK-StRegG § 8 Rz 1 und 14).

Betreffend das Recht der betroffenen Person, vom Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wird darauf hingewiesen, dass im Verfahren nach § 8 StRegG auch die Feststellung beantragt werden kann, dass die Tilgung der Verurteilung nach dem TilgG (bereits) eingetreten ist. Ist dies der Fall, darf sie nicht mehr in der Strafregisterauskunft oder Strafregisterbescheinigung aufscheinen. Auch wenn dies das Gesetz nicht ausdrücklich vorsieht, kann laut höchstgerichtlicher Judikatur mit einem Antrag nach § 8 StRegG auch die Feststellung begehrt werden, dass eine Verurteilung der Beschränkung der Auskunft gemäß § 6 TilgG unterliegt (vgl. VwGH 99/01/0453).

Da sich der Anwendungsbereich der Art. 16 bis 18 der Datenschutz-Grundverordnung mit jenem des § 8 StRegG deckt, soll es nicht erforderlich sein, dass sich der Betroffene in seinem Antrag gemäß § 8 StRegG auch noch zusätzlich auf die Datenschutz-Grundverordnung stützt.

Erst wenn dem Antrag nach Abschluss des Feststellungverfahrens ganz oder teilweise Folge gegeben wird, ist das Strafregister gemäß Abs. 3 zu berichtigen, d.h. der Eintrag richtigzustellen bzw. zu löschen oder die Datenverarbeitung einzuschränken. Demzufolge kommt dem Feststellungsbescheid konstitutive Wirkung zu. Andererseits würden – sofern der Betroffene die Einschränkung der Verarbeitung verlangt (vgl. Art. 18 Abs. 1 lit. a der Datenschutz-Grundverordnung) – die bestrittenen Daten bis zum Abschluss des Feststellungsverfahrens nicht im Strafregister aufscheinen, was insbesondere die Möglichkeit der Beurteilung der Vertrauenswürdigkeit von Personen (zB Sicherheitsüberprüfungen bzw. Gefährderprognosen) vollständig konterkarieren und eine Missbrauchsgefahr mit sich bringen würde. Es kann dem Betroffenen nicht überlassen sein, durch die Ausübung dieser Rechte etwa zu verhindern, dass Behörden oder sonstige Stellen über Eintragungen im Strafregister informiert werden dürfen. Die geplante Beschränkung hat auch kein Rechtsschutzdefizit zur Folge: Basis für die Eintragung bildet ein in einem rechtsstaatlichen Verfahren ergangenes rechtskräftiges Urteil, wobei der Betroffene bereits im Strafverfahren die Möglichkeit hatte, den Instanzenzug auszuschöpfen.

Das in Abs. 1 geregelte Rechtsschutzverfahren gegen Aufnahmen in das Strafregister soll – wie bisher – keine Anwendung auf Eintragungen rechtskräftiger Verurteilungen österreichischer Staatsbürger durch Strafgerichte anderer Mitgliedstaaten und die mit diesen Verurteilungen zusammenhängenden Informationen, die gemäß § 2 Abs. 1 Z 9 StRegG ausschließlich zum Zweck der Übermittlung eines Anhangs zu einer Strafregisterauskunft bereitgehalten werden, finden. Hinsichtlich der Aufnahme dieser Einträge in den Anhang kommt Österreich keine Auswahlbefugnis zu, auch deren Löschung richtet sich nach dem jeweiligen Recht des Urteilsstaates. Damit unterliegen die gemäß § 2 Abs. 1 Z 9 StRegG gespeicherten Einträge auch nicht dem Rechtsschutz des § 8 StRegG. Anträge auf Richtigstellung und Löschung hinsichtlich dieser Daten sind demnach an die zuständigen Behörden des Urteilsstaates zu richten (vgl. 1677 BlgNR 23. GP zu BGBl. I Nr. 29/2012).

Gemäß Art. 21 Abs. 1 der Datenschutz-Grundverordnung hat der Betroffene zudem das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten Widerspruch zu erheben. Ein solches, dem Betroffenen durch die Datenschutz-Grundverordnung in genereller Weise eingeräumtes Widerspruchsrecht kann jedoch gemäß Art. 23 der Datenschutz-Grundverordnung 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. Die in dieser Bestimmung genannten Gründe für die Zulässigkeit des Ausschlusses dieser Rechte sind auch vor dem Hintergrund der im Verfassungsrang stehenden Bestimmung des § 1 Abs. 2 DSG zu sehen, wonach Eingriffe einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 EMRK genannten Gründen zulässig sind, vorgenommen werden dürfen. Danach ist ein Eingriff einer staatlichen Behörde nur dann statthaft, wenn dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. Damit zeigt sich, dass gesetzlich vorgesehene Eingriffe, die im Einklang mit der Verfassung stehen, jedenfalls die Voraussetzungen mit sich bringen, die für die Zulässigkeit einer Beschränkung gemäß Art. 23 Abs. 1 der Datenschutz-Grundverordnung erforderlich sind. Von einer solchen möglichen Beschränkung wird in Abs. 5 für sämtliche nach dem StRegG verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten, sparsamen und effizienten Vollzug des StRegG sowie die Funktionalität des Strafregisters ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 der Datenschutz-Grundverordnung für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 der Datenschutz-Grundverordnung vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d der Datenschutz-Grundverordnung). Durch die Ausübung des Widerspruchsrechts – das auch nach bisheriger Rechtslage nicht vorgesehen ist – könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben nicht verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von im Strafregister aufscheinenden Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (siehe auch Art. 23 Abs. 1 lit. h der Datenschutz-Grundverordnung) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich.

Würde das Widerspruchsrecht zur Anwendung gelangen, würde dies dazu führen, dass eine Vielzahl der im Strafregister aufscheinenden Personen einer Verarbeitung der Verurteilungen widersprechen würden, was einen beträchtlichen Verwaltungsaufwand zur Folge hätte und den Vollzug wesentlich beeinträchtigen würde, weil im jeweiligen Einzelfall geklärt werden müsste, dass die Interessen des Verantwortlichen an der Datenverarbeitung jenen des Betroffenen überwiegen. Im Falle eines Widerspruchs wäre nicht mehr gewährleistet, dass sämtliche strafrechtlich relevanten Daten tatsächlich im Strafregister aufscheinen, was den Zweck des Strafregisters – die Evidenthaltung strafrechtlicher Verurteilungen zum Zwecke der Strafrechtspflege und inneren Sicherheit – vollständig konterkarieren würde. Dies würde dazu führen, dass etwa Gerichte oder sonstige Behörden nicht sämtliche Daten und Informationen, die diese für eine rechtsrichtige Entscheidung sowie zu Strafbemessungszwecken benötigen, tatsächlich heranziehen können und könnte dies – vor allem bei Gefahr im Verzug (Gewalt in der Familie, notwendige Einstufung der Gefährlichkeit einer Person etc.) – in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren. Es darf dem Betroffenen nicht möglich sein, durch die (unbeschränkte) Ausübung dieser Rechte zu verhindern, dass Daten weiterhin verarbeitet werden dürfen. Der generelle Ausschluss des Widerspruchsrechts ist daher unerlässlich.

Den für den Ausschluss des Widerspruchsrechts einschlägigen Vorgaben des Art. 23 Abs. 2 der Datenschutz-Grundverordnung wird entsprechend Rechnung getragen. So ergeben sich aus den gesetzlichen Vorgaben zur Verarbeitung von personenbezogenen Daten nach diesem Bundesgesetz für den Ausschluss des Widerspruchsrechts insbesondere sowohl der Umfang der vorgenommenen Beschränkung und die Kategorien der betreffenden personenbezogenen Daten als auch der für deren Verarbeitung Verantwortliche und die Zwecke. 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 unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, 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, Löschung und Einschränkung der Verarbeitung gemäß den Art. 16 bis 18 der Datenschutz-Grundverordnung im Rahmen des Feststellungsverfahrens gemäß § 8 StRegG Gebrauch zu machen. Durch den Ausschluss dieses Rechts entsteht für den Betroffenen daher auch kein Rechtsschutzdefizit.

Als grundrechtsschützende Maßnahme und in Umsetzung des Art. 23 Abs. 2 lit. h der Datenschutz-Grundverordnung ist im letzten Satz vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind. Ausdrücklich steht es der Verantwortlichen 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 der Homepage).

Diese Ausführungen lassen erkennen, dass das in der Datenschutz-Grundverordnung vorgesehene Recht auf Widerspruch in einem Spannungsverhältnis zur gesetzlich angeordneten Datenverarbeitung steht. 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 des Strafregisterwesens und Anwendbarkeit des StRegG sowie die Funktionalität und die ordnungsgemäße Führung des Strafregisters gewährleisten.

Zu Z 5 bis 7 (§ 9 Abs. 1 Z 2a und 2b und § 9a Abs. 1 Z 5 und 6 StRegG):

Die Voraussetzungen für Übermittlungen personenbezogener Daten an Drittländer werden in Kapitel V der Datenschutz-Grundverordnung festgelegt. Aus diesem Grund sollen die vorgeschlagenen Regelungen in § 9 und § 9a StRegG künftig differenzieren, je nachdem, ob sie Behörden aus Mitgliedstaaten der Europäischen Union oder Drittstaaten betreffen.

Hinsichtlich der Strafregisterauskünfte an Behörden aus Drittstaaten sowie Sonderauskünfte zu Sexualstraftätern an Gerichte, Staatsanwaltschaften und Sicherheitsbehörden aus Drittstaaten in Strafverfahren soll demzufolge betreffend die näheren Voraussetzungen lediglich ein Verweis auf die Datenschutz-Grundverordnung aufgenommen werden.

Zu Z 8 und 9 (§ 10 Abs. 1a und 4 StRegG):

Im Hinblick darauf, dass Auskünfte gemäß Art. 15 der Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen (dazu gleich unten) und vor dem Hintergrund von Art. 12 Abs. 5 der Datenschutz-Grundverordnung soll der letzte Satz in § 10 Abs. 1a StRegG entfallen.

Art. 23 der Datenschutz-Grundverordnung ermächtigt die Union und die Mitgliedstaaten dazu, bestimmte Pflichten und Rechte, darunter auch das Auskunftsrecht gemäß Art. 15 der Datenschutz-Grundverordnung, durch „Gesetzgebungsmaßnahmen“ zu beschränken, sofern gewisse näher normierte Gründe vorliegen (siehe auch die Erläuterungen zu § 8 StRegG). Diese Bestimmung enthält somit eine Öffnungsklausel, die einer gesetzlichen Maßnahme der Mitgliedstaaten zugänglich ist. Zum Schutz des Betroffenen (vgl. Art. 23 Abs. 1 lit. i der Datenschutz-Grundverordnung) soll das Recht auf Auskunft insoweit gesetzlich beschränkt werden, als Auskünfte gemäß Art. 15 der Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen.

Mit der Tilgung der Verurteilung erlöschen alle nachteiligen Folgen, die kraft Gesetzes mit der Verurteilung verbunden sind. Ist eine Verurteilung getilgt, so gilt der Verurteilte fortan als gerichtlich unbescholten und ist auch nicht verpflichtet, die getilgte Verurteilung anzugeben (vgl. § 1 TilgG). Das Strafregister dient zwar in vielen Bereichen der Beurteilung der Verlässlichkeit einer Person, wie für die Ausübung gefahrengeneigter Tätigkeiten (zB Gebrauch von Waffen und Sprengmitteln). Mit der Tilgung der Verurteilung soll es dem Verurteilten jedoch ermöglicht werden, nach einer gewissen Zeit des Wohlverhaltens wieder die Stellung eines Unbestraften zu erhalten. Sie soll demzufolge die Gefahr hintanhalten, dass frühere Verurteilungen, die bereits lange Zeit zurückliegen, bekannt werden und eine Wiedereingliederung des Täters in die Gesellschaft und die Arbeitswelt be- und verhindern (vgl. *Kert* in *Fuchs/Ratz*, WK-TilgG Vor Rz 5ff). Das Instrument der Auskunftsbeschränkung gemäß § 6 TilgG bietet ebenfalls den Vorteil, dass durch die weitgehende Einschränkung der Publizität der Verurteilungen die Resozialisierung des Täters erleichtert wird. Sie soll dem Betroffenen ermöglichen, gegenüber Dritten als unbescholten auftreten zu können. Nur dort, wo es die öffentliche Sicherheit erfordert, soll eine Auskunft über alle Verurteilungen gegeben werden, wie dies z. B. gegenüber Gerichten, Staatsanwaltschaften, Sicherheitsbehörden sowie bestimmten anderen Behörden der Fall ist. Der Verurteilte ist nicht verpflichtet, die Verurteilung gegenüber Behörden oder Privaten anzugeben.

Durch die Aufhebung der Regelung in § 26 Abs. 9 DSG 2000, wonach für Auskünfte aus dem Strafregister die besonderen Bestimmungen des StRegG über Strafregisterbescheinigungen gelten, durch das Datenschutz-Anpassungsgesetz 2018 würde die Gefahr bestehen, dass z. B. Dienstgeber oder andere Stellen die oben erwähnten Auskunftsbeschränkungen dadurch umgehen, dass anstelle einer Strafregisterbescheinigung die Beibringung eines Auskunftsbegehrens über sämtliche verarbeitete Daten gemäß Art. 15 der Datenschutz-Grundverordnung verlangt wird. Das Telos von Tilgung und Auskunftsbeschränkung, d.h. Beseitigung der Stigmatisierung und Erleichterung der Resozialisierung, würde demnach ins Leere gehen. Dem soll die Regelung in § 19 Abs. 4 StRegG entgegenwirken, indem zum Schutz des Betroffenen Auskünfte gemäß Art. 15 der Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen und somit wie bisher weder getilgte Verurteilungen (§ 1 Abs. 5 TilgG) noch Verurteilungen, die einer Auskunftsbeschränkung unterliegen (§ 6 Abs. 4 TilgG), in diese Auskunft aufgenommen, noch darin auf irgendeine Art ersichtlich gemacht werden dürfen.

In Bezug auf die Ablehnungsgründe in Abs. 3 ist darauf hinzuweisen, dass auch die Datenschutz-Grundverordnung den Identitätsnachweis des Betroffenen zur Inanspruchnahme seiner Rechte als zulässig erachtet (vgl. Art. 12 Abs. 6 bzw. EG 64 der Datenschutz-Grundverordnung). Der Antrag ist auch dann abzulehnen, wenn nach dem Antragsteller zum Zwecke der Aufenthaltsermittlung, Verhaftung oder Festnahme gefahndet wird. Der Bestimmung liegt die Überlegung zugrunde, dass es rechtspolitisch nicht vertretbar erscheint, dass derselbe Staat, der nach einer Person, die sich einer im Inland anhängigen

Strafverfolgung oder -vollstreckung offenbar zu entziehen versucht, fahndet, derselben Person einen untadeligen Lebenswandel bescheinigt (ErläutRV 817 BlgNR 11. GP 11). Der Einschränkung liegt demnach ein wichtiges Ziel des allgemeinen öffentlichen Interesses gemäß Art. 23 Abs. 1 lit. e der Datenschutz-Grundverordnung zugrunde.

Art. 12 Abs. 5 der Datenschutz-Grundverordnung gilt gleichermaßen.

Zu Z 10 bis 14 und 19 (§ 10a Abs. 1 und 3, § 10b Abs. 1 und 2, § 11 Abs. 6 und § 14a Abs. 1 StRegG):

Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im StRegG verwendeten Begriffe erforderlich erscheint, werden diese nun an die Definitionen der Datenschutz-Grundverordnung (Art. 4) angeglichen. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 der Datenschutz-Grundverordnung beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Zudem sollen im Sinne der neuen datenschutzrechtlichen Terminologie beispielsweise die Begriffe „Übersendung“, „Mitteilung“, „Bekanntgabe“ oder „Weiterleitung“ von Daten durch das Wort „Übermittlung“ ersetzt werden.

Zu Z 15 und 16 (§ 12 StRegG):

§ 14 DSG 2000 sieht unter anderem vor, dass Protokolldaten über tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen drei Jahre lang aufbewahren sind, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. Infolge des Entfalls des bisherigen § 14 DSG 2000 durch das Datenschutz-Anpassungsgesetz 2018 und den Umstand, dass die Datenschutz-Grundverordnung von spezifischen Regelungen betreffend die Protokollierung Abstand nimmt, wird vorgeschlagen, den – für Zwecke der Sicherheitspolizei einschlägigen – § 50 DSG, wonach aus den Protokolldaten auch die Identität eines allfälligen Empfängers verarbeiteter personenbezogener Daten hervorgehen muss, auf die Protokollierung von Datenverarbeitungsvorgängen im Rahmen des Strafregisters für anwendbar zu erklären. Die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren soll beibehalten werden.

Zu Z 17 (§ 13a StRegG):

Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken verarbeitet, können bei Vorliegen näher bestimmter Voraussetzungen gemäß Art. 89 Abs. 2 der Datenschutz-Grundverordnung – vorbehaltlich der Bedingungen und Garantien gemäß Abs. 1 – durch nationales Recht Ausnahmen von den Rechten gemäß Art. 15 (Auskunftsrecht der betroffenen Person), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) vorgenommen werden. Da es in der Praxis kaum möglich wäre, gegenüber Betroffenen bei wissenschaftlichen Erhebungen aufgrund der Vielzahl, Vielfalt und des Umfangs der betroffenen personenbezogenen Daten sämtliche dieser Rechte zu wahren bzw. die Wahrung der Betroffenenrechte die Verwirklichung der spezifischen wissenschaftliche Zwecke ernsthaft beeinträchtigen, wenn nicht sogar unmöglich machen würde, soll die Ausnahmeermächtigung gemäß Art. 89 Abs. 2 der Datenschutz-Grundverordnung betreffend die im Strafregister gespeicherten Daten in Anspruch genommen werden.

Demzufolge soll, soweit personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken übermittelt werden, dem Betroffenen das Recht auf Auskunft gemäß Art. 15 der Datenschutz-Grundverordnung nicht zukommen. Da bei Datenverarbeitungen für im öffentlichen Interesse liegenden Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke personenbezogene Daten, die nicht unter § 7 Abs. 1 DSG idF des Datenschutz-Anpassungsgesetzes 2018 fallen, nur verarbeitet werden dürfen, wenn dies entweder gesetzlich vorgesehen ist, eine Einwilligung der betroffenen Person erteilt wurde oder eine Genehmigung der Datenschutzbehörde vorliegt (vgl. § 7 Abs. 2 DSG), ist der Ausschluss dieses Rechts bei Übermittlungen jedenfalls gerechtfertigt und steht dieser – auch aufgrund der eingeschränkten Ausgestaltung – im Einklang mit den Vorgaben der Datenschutz-Grundverordnung. Die weitere Verarbeitung der Daten zu den genannten Zwecken ist hingegen nicht Gegenstand dieser Bestimmung.

Im Sinne der neuen datenschutzrechtlichen Terminologie soll ferner der Begriff der „Bekanntgabe“ durch jenen der „Übermittlung“ ersetzt werden.

Zu Z 18 (§ 14 Abs. 14 StRegG):

Die Bestimmung regelt das Inkrafttreten.

Zu Art. 113 (Änderung des Strafvollzugsgesetzes):

Zu Z 1 (§§ 9 Abs. 5, 10 Abs. 1, 13, 14 Abs. 1 und 3, 14a Abs. 1, Abs. 2 Z 2 und Abs. 3, 15c Abs. 1, 16a Abs. 1 Z 2 und 3, 24 Abs. 3, 52 Abs. 2, 69 Abs. 1, 78 Abs. 1 und 2, 80 Abs. 2, 84 Abs. 1 und 3, 97, 101 Abs. 2 und 3, 106 Abs. 3, 116 Abs. 1, 121 Abs. 5, 121b Abs. 4, 134 Abs. 1 und 6, 135 Abs. 2, 161 sowie 179a Abs. 1 und 3 StVG), 5 (§§ 18a Abs. 3, 99 Abs. 5a und 156b Abs. 2 StVG), 6 (§ 156b Abs. 3 StVG) und 8 (§ 182 StVG):

Mit den vorgeschlagenen Änderungen soll die Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, soweit hier relevant, nachvollzogen werden. Dies betrifft vor allem die Erweiterung des Bundesministeriums für Justiz zum Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. Im Bereich der Vollziehungsbestimmung des § 182 StVG ist überdies nunmehr sowohl hinsichtlich der Arbeit der Strafgefangenen (§§ 44 bis 55 StVG) und der sozialen Fürsorge (§§ 75 bis 84) als auch hinsichtlich der ärztlichen Betreuung (§§ 66 bis 74) und der Unterbringung in Anstalten für geistig abnorme Rechtsbrecher sowie in Anstalten für entwöhnungsbedürftige Rechtsbrecher (§§ 164 bis 170 StVG) gegebenenfalls das Einvernehmen mit dem Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz herzustellen.

Zu Z 2 (§ 15a StVG):

Abs. 1 bildet die Rechtsgrundlage für die Verarbeitung (bisher: Verwendung) personenbezogener Daten (§ 38 DSG idF BGBl. I Nr. 120/2017), einschließlich der bisher als „sensible Daten“ bezeichneten „besonderen Kategorien personenbezogener Daten“ im Sinne des § 39 DSG idF BGBl. I Nr. 120/2017 in Bezug auf die Insassen der Justizanstalten. Nach der zuletzt genannten Bestimmung ist die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person für u.a. die Zwecke der Verhütung von Straftaten sowie der Strafvollstreckung zwar zulässig, jedoch nur dann, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden. Überdies muss die Verarbeitung – sofern sie sich nicht auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat – nach § 38 DSG idF BGBl. I Nr. 120/2017 zulässig sein; dies bedeutet, dass die Verarbeitung der personenbezogenen Daten grundsätzlich gesetzlich vorgesehen, für die Erfüllung einer Aufgabe wie der Verhütung von Straftaten oder der Strafvollstreckung erforderlich und verhältnismäßig sein muss. § 15a Abs. 1 übernimmt diese Kautelen.

Abs. 2 erfasst alle jene Personen, bei denen – abgesehen von den in Abs. 1 geregelten Insassen der Justizanstalten – die Verarbeitung personenbezogener zur Erfüllung der Aufgaben der Vollzugsverwaltung erforderlich sein kann (§ 38 DSG idF BGBl. I Nr. 120/2017). Dieses Erfordernis kann sich situationsbedingt (z. B. aus Anlass einer Besichtigung oder im Rahmen der Z 4), aber auch bei grundsätzlich länger andauerndem Kontakt zu einem Insassen oder der Vollzugsverwaltung ergeben (z. B. regelmäßige Besuche, Zulieferer). Gegenüber dem Ministerialentwurf sollen – wenngleich dieser Personenkreis auch schon als von den im Abs. 1 genannten Daten umfasst angesehen werden könnte – ausdrücklich auch die Daten jener Personen angeführt werden, mit denen ein Strafgefangener im Rahmen des elektronisch überwachten Hausarrests in Kontakt tritt (Abs. 2 Z 5). Es handelt sich dabei im Wesentlichen um die Daten des Bereitstellers einer Unterkunft (etwa Vermieters nach § 156c Abs. 1 Z 2 lit. a StVG), des Arbeitgebers (§ 156c Abs. 1 Z 2 lit. b StVG), der Mitbewohner (§ 156c Abs. 1 Z 3 StVG) und allfälliger externer Personen nach § 3 Z 5 HausarrestV.

Soweit die betroffenen Personen die Anstalt betreten, kann auch die Verarbeitung biometrischer Daten, die zu den besonderen Kategorien personenbezogener Daten nach § 39 DSG idF BGBl. I Nr. 120/2017 zählen, erforderlich sein. Abs. 2 berücksichtigt gleichfalls die Kautelen der §§ 38 und 39 DSG idF BGBl. I Nr. 120/2017.

Abs. 3 regelt die Aufteilung der Aufgaben und Pflichten der gemeinsamen Verantwortlichen. Hinsichtlich zentraler Datenanwendungen, die den Vollzugsbehörden erster Instanz vom Bundesministerium für Justiz zur Nutzung zur Verfügung gestellt/vorgegeben und im Wege eines bundesweit einheitlich vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz herangezogenen Auftragsverarbeiters infrastrukturell (Hardware, Software, Applikationen) betreut werden (zB IVV, IWV etc.), werden die Pflichten des Verantwortlichen nach den §§ 46 DSG idF BGBl. I Nr. 120/2017 (Art. 24 DSGVO Abs. 1 und Abs. 2 [technische und organisatorische Datenschutzmaßnahmen] bzw. Art. 25

Abs. 1 und Abs. 2 [Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen]), § 49 DSG idF BGBl. I Nr. 120/2017 (Verzeichnis der Verarbeitungstätigkeiten), § 52 DSG idF BGBl. I Nr. 120/2017 (Datenschutz-Folgenabschätzung) und 54 DSG idF BGBl. I Nr. 120/2017 (Datensicherheitsmaßnahmen) vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz wahrgenommen. Die zentralen Datenanwendungen werden in den Verzeichnissen der Verarbeitungstätigkeiten sowohl des Bundesministeriums für Justiz als auch der Vollzugsbehörden erster Instanz aufgenommen. Andere, von den Vollzugsbehörden erster Instanz lokal betriebene Datenanwendungen sind zusätzlich in deren Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Die Wahrnehmung der Pflichten der Verantwortlichen hinsichtlich jener Datenanwendungen, die die Vollzugsbehörden erster Instanz aus eigenem lokal betreiben, obliegt den Justizanstalten. Ebenso obliegt den Vollzugsbehörden erster Instanz hinsichtlich sämtlicher Datenanwendungen (zentrale und insbesondere lokale Datenanwendungen) die Wahrnehmung der Rechte der betroffenen Personen nach den §§ 42 bis 45 DSG idF BGBl. I Nr. 120/2017 (das sind iW Informations- und Auskunftsrechte sowie gegebenenfalls das Recht auf Richtigstellung oder Löschung bzw. Einschränkung der Verarbeitung).

Die Abs. 4 und 5 entsprechen iW den bisherigen Abs. 3 und 4, wobei an die Stelle des bisherigen „Dienstleisters“ der „Auftragsverarbeiter“ und an die Stelle des „Auftraggebers“ der „Verantwortliche“ tritt.

Zu Z 3 (§ 15b StVG):

Da das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz Kompetenzen als oberste Vollzugsbehörde wahrnimmt (§ 13 StVG), während die AnstaltsleiterInnen Vollzugsbehörden erster Instanz sind (§ 11 StVG), soll die Differenzierung wo nicht sachlich geboten aufgehoben und stattdessen der einheitliche Begriff „Vollzugsbehörden“ verwendet werden. Die Erweiterung der Datenübermittlungsstellen um jenen „kraft Vereinbarung“ soll dem Umstand Rechnung tragen, dass im Forschungskontext in vertragliche Vereinbarungen mit externen Forschungspartnern üblicherweise auch Datenverarbeitungsvorgaben festgelegt werden. Mit dem letzten Satz des Abs 1 soll eine den Aktualitätsvorgaben des § 37 Abs. 1 Z 4 und Abs. 6 DSG idF BGBl. I Nr. 120/2017 entsprechende Regelung in das StVG aufgenommen werden.

Abs. 2 dient der „Umsetzung“ des § 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017 für die Zwecke des Strafvollzuges (vgl. für die Strafverfolgung die Ausführungen in den Gesetzesmaterialien zum Datenschutz-Anpassungsgesetz 2018, 1664 BlgNR XXV. GP, 19 = 1761 BlgNR XXV. GP, 31 f.). im Strafvollzugskontext kann sich ein entsprechender Anwendungsfall etwa bei der Weiterverarbeitung der aus Anlass des ersten Vollzuges einer Straf- oder Untersuchungshaft aufgenommenen Insassendaten für eine im unmittelbaren Anschluss nachfolgende Straf- oder Untersuchungshaft, sei es durch die datenerstverarbeitende Vollzugsbehörde oder eine z. B. im Wege der Klassifizierung (§ 134 StVG) oder Strafvollzugsortsänderung (§ 10 StVG, § 183 StPO) neu zuständige Vollzugsbehörde. Zur Rechtsgrundlage für eine Weiterverarbeitung vormalig verarbeiteter Insassendaten im Falle neuerlicher Inhaftierung nach zwischenzeitiger Enthaftung oder Entlassung siehe Art. 13 Z 4 des Entwurfs (§ 15c Abs.3).

Abs. 3 entspricht im Wesentlichen dem geltenden Abs. 2. Unter einem dient diese Bestimmung auch als Grundlage für die Verarbeitung der von den Sicherheitsbehörden im Rahmen ihrer Zuständigkeit gemäß § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 verarbeiteten Personendaten durch die Vollzugsbehörden für ihre im Rahmen des § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 notwendigen Zwecke (§ 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017).

Abs. 4 entspricht mit umgekehrten Vorzeichen der Regelung des Abs 3. Wird eine Person von der Vollzugsverwaltung an eine Sicherheitsbehörde oder eine sicherheitsbehördliche Hafteinrichtung übergeben, gründet die datenschutzrechtliche Verarbeitungszuständigkeit auf § 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017. Nun existiert zwar bereits eine vergleichbare Bestimmung in Form des § 58b Abs 3 SPG. Da aber Insassen aus Justizanstalten nach ihrer justiziellen Anhaltung oftmals zu *fremden*polizeilichen Haftzwecken, deren Datenverarbeitungsgrundlage in der DSGVO gründet (und nicht durch die Zwecke des § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 abgedeckt scheint), an die polizeilichen Behörden übergeben werden, soll für die Zulässigkeit der Datenübermittlung aus der Sphäre der Vollzugsbehörden in die Sphäre der Fremdenbehörden im Sinne des § 40 Abs. 2 DSG idF BGBl. I Nr. 120/2017 eine ausdrückliche gesetzliche Grundlage geschaffen werden.

Zu Z 4 (§ 15c StVG):

§ 15c regelt idgF den eingeschränkten Datenzugriff bzw. die Löschung von Insassendaten. Insoweit kann die Bestimmung im Wesentlichen unverändert bleiben. Es soll lediglich eine Löschungsvorschrift hinsichtlich der verarbeiteten personenbezogener Daten jener Personen, die keine Insassen sind (siehe dazu bei § 15a Abs. 2 StVG in der Fassung des Entwurfs), angefügt werden, die unter Berücksichtigung

des sachlichen und verfahrensökonomischen Bedarfes der Vollzugsverwaltung – und § 37 Abs. 1 Z 5 DSG idF BGBl. I Nr. 120/2017 entsprechend – gestaffelt festgesetzt werden sollen.

Zu Art. 114 (Änderung der ZPO):

Zu § 219 ZPO:

Mit der vorgeschlagenen Bestimmung soll die Umschreibung der im „öffentlichen Interesse“ zu berücksichtigenden Aspekte im Zuge der gemäß § 219 Abs. 2 ZPO zu treffenden Interessenabwägung an die in Art. 23 Abs. 1 DSGVG getroffene Wertung angepasst werden.

Zum 9. Hauptstück (Landesverteidigung)

Allgemeines

Hauptgesichtspunkte des Entwurfes:

Die Datenschutz-Grundverordnung findet gemäß ihrem Art. 2 Abs. 2 lit. a *keine Anwendung* auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrecht fällt (dazu zählen insbesondere auch Tätigkeiten im Interesse der *nationalen Sicherheit* – vgl. Erwägungsgrund Nr. 16 zur DSGVO bzw. Art. 4 Abs. 2 EUV).

Nach § 4 Abs. 1 des Datenschutzgesetzes (DSG) in der mit 25. Mai 2018 in Kraft tretenden Fassung finden die Bestimmungen der Datenschutz-Grundverordnung jedoch indirekt auch für den Bereich der nationalen Sicherheit Anwendung, soweit dies die Bestimmungen des 3. Hauptstücks des Datenschutzgesetzes vorsehen.

Für die Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit gelten unter Bedachtnahme auf § 4 Abs. 1 DSG jene Bestimmungen der Datenschutz-Grundverordnung, die in den spezifischen Bestimmungen des 3. Hauptstückes DSG übernommen werden. Im Hinblick auf den, aus der Lehre und Judikatur ableitbaren, weiten Inhalt des Rechtsbegriffes „nationale Sicherheit“ wird davon auszugehen sein, dass alle unmittelbar der „militärischen Landesverteidigung“ (Art. 79 Abs. 1 B-VG) dienenden Datenverarbeitungen dem entsprechenden Ausnahmetatbestand unterliegen werden. Da Angelegenheiten der nationalen Sicherheit nicht dem Unionsrecht unterliegen (vgl. Art. 2 Abs. 2 lit. a iVm Erwägungsgrund Nr. 16 zur DSGVO bzw. Art. 4 Abs. 2 EUV), kommt diesbezüglich auch das europarechtliche Transformationsverbot nicht zur Anwendung; daher wurde das Kapitel III DSGVO „Rechte der betroffenen Person“ in den 2. Abschnitt des 3. Hauptstückes DSG transformiert und dort – unter anderem auch für den Bereich der nationalen Sicherheit – abschließend geregelt. Daher wird weiters davon auszugehen sein, dass Bestimmungen des Kapitels III DSGVO, welche nicht in den 2. Abschnitt des 3. Hauptstückes DSG transformiert wurden, für den Bereich der nationalen Sicherheit nicht zur Anwendung gelangen, wie zB das Widerspruchsrecht nach Art. 21 DSGVO. Materienspezifische Sondernormen über die Verarbeitung personenbezogener Daten bleiben jedenfalls unberührt und gehen als leges speciales auch den Bestimmungen des 3. Hauptstückes DSG vor (§ 69 Abs. 8 DSG).

Mit dem vorliegenden Gesetzesvorschlag sollen die im Wehrrecht bestehenden datenschutzrechtlichen Bestimmungen an die ab 25. Mai 2018 geltende Rechtslage angepasst werden.

Die mit der Vollziehung des jeweiligen Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem jeweiligen Materiengesetz. Als Verantwortliche im Sinne des 3. Hauptstückes des Datenschutzgesetzes werden daher der Bundesminister für Landesverteidigung sowie die jeweiligen Behördenleiter im Rahmen der ihnen übertragenen Aufgaben zu verstehen sein.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich aus Art. 10 Abs. 1 Z 15 B-VG („militärische Angelegenheiten“).

Zu Art. 117 (Änderung des Wehrgesetzes 2001):

Zu Z 1 bis 6 (Inhaltsverzeichnis zu § 55a, § 38 Abs. 2, § 39 Abs. 1, die Überschrift zu § 55a sowie § 55a Abs. 1 und 1a):

Auf Grund des Datenschutz-Anpassungsgesetzes 2018 wurden die Begriffe „Daten“ und „Verwenden von Daten“ nach dem DSG 2000 durch die Begriffe „personenbezogene Daten“ bzw. „Verarbeitung“ von Daten nach § 36 Abs. 2 Z 1 und 2 DSG ersetzt. Vor diesem Hintergrund wären auch die in Rede stehenden Bestimmungen entsprechend anzupassen. In diesem Zusammenhang wird auch der Begriff „Verarbeitung“ von Daten nicht mehr wie bisher im Sinne des § 4 Z 9 DSG 2000 sondern nunmehr im Sinne des § 36 Abs. 2 Z 2 DSG zu verstehen sein.

Nach § 38 DSG ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn sie gesetzlich vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist. Den Vorgaben des § 1 Abs. 2 DSG und der einschlägigen Judikatur des Verfassungsgerichtshofes entsprechend sollen daher die in Rede stehenden Datenschutzregelungen ausreichend präzise regeln, wer welche personenbezogenen Daten für welche Zwecke verarbeiten darf. Die Verarbeitung dieser Daten soll darüber hinaus nur zulässig sein, wenn dies zur Erfüllung der jeweils übertragenen Aufgabe durch die Behörde im Einzelfall erforderlich ist. In § 55a Abs. 1 werden die erforderlichen Daten zu Datenkategorien zusammengefasst, wobei hinsichtlich der Grunddaten sowie der Gesundheitsdaten im Hinblick auf deren besondere Sensibilität und der damit verbundenen höheren Anforderung an den Determinierungsgrad bei Eingriffen staatlicher Behörden in das Grundrecht auf Datenschutz nach § 1 DSG auf Grund von Gesetzen eine taxative Nennung geboten erscheint. Hinsichtlich der übrigen Datenkategorien wird von einer taxativen Aufzählung der in jedem Verwaltungsverfahren nach diesem Bundesgesetz erforderlichen Daten auf Grund der Unvorhersehbarkeit und Vielzahl an möglichen Fällen Abstand genommen (zB sind die Gründe für eine Befreiung vom Präsenzdienst nach § 26 Abs. 1 aus familiären oder wirtschaftlichen Gründen ex ante kaum bestimmbar).

Der primäre Zweck der wehrrechtlichen Datenverarbeitung liegt in der Sicherstellung der verfassungsgesetzlich normierten allgemeinen Wehrpflicht männlicher Staatsbürger (Art. 9a Abs. 3 B-VG). Die konkreten Teilelemente der Wehrpflicht ergeben sich aus einfachgesetzlichen Bestimmungen, insbesondere aus dem Wehrgesetz 2001. So ist die Dauer der Wehrpflicht in § 10 WG 2001 festgelegt und erstreckt sich grundsätzlich bis zur Vollendung des 50. Lebensjahres, kann jedoch für bestimmte Gruppen von Wehrpflichtigen bis zum vollendeten 65. Lebensjahr und in Einzelfällen auch darüber hinaus bestehen. Damit wird auch die Dauer einer rechtmäßigen Datenverarbeitung im Sinne des § 37 Abs. 1 Z 5 DSG festgelegt. Die konkreten Pflichten, die sich aus der Wehrpflicht ergeben, sind in § 11 WG 2001 näher umschrieben und umfassen

- die Stellungspflicht,
- die Pflicht zur Leistung des Präsenzdienstes,
- die Pflichten des Milizstandes,
- bestimmte Melde- und Bewilligungspflichten sowie
- bestimmte Verschwiegenheitspflichten.

Daraus ergibt sich die Notwendigkeit zur Verarbeitung bestimmter Datenarten, die im vorliegenden Entwurf aufgezählt sind.

Unter „Grunddaten“ werden jene Daten zu verstehen sein, die in erster Linie zur Identifizierung einer Person erforderlich sind, wie das bereichsspezifische Personenkennzeichen (bPK) nach § 9 des E-Government-Gesetzes (E-GovG), BGBl. I Nr. 10/2004. Unter Kontaktdaten werden Abgabestellen und elektronische Zustelladressen im Sinne des Zustellgesetzes, BGBl. Nr. 200/1982, sowie die Telefonnummer der betroffenen Person zu verstehen sein. Daten über die gesetzlichen Vertreter sind vor allem für jene Fälle erforderlich, in denen die betroffene Person auf Grund ihrer Minderjährigkeit der Mitwirkung der gesetzlichen Vertreter bedarf (vgl. § 57). Die Verarbeitung des Religionsbekenntnisses dient ausschließlich zur religiösen Betreuung der betroffenen Personen, zB durch die Militärseelsorge oder zur Berücksichtigung religiöser Ernährungsvorschriften während des Wehrdienstes, sofern die betroffenen Personen dazu ausdrücklich ihre Einwilligung erteilt haben.

Der Begriff „Gesundheitsdaten“ ist der Regelung § 36 Abs. 2 Z 14 DSG nachgebildet. Diese Daten gelten als „besondere Kategorie personenbezogener Daten“ im Sinne des § 39 DSG und werden insbesondere im Rahmen der Feststellung der körperlichen und geistigen Eignung zum Wehrdienst (Stellung) bzw. im Rahmen anderer Eignungsfeststellungen (zB für den Auslandseinsatzpräsenzdienst) sowie im Rahmen eines Wehrdienstes über den körperlichen und geistigen Gesundheitszustand einer Person erhoben (Dienstfähigkeitsuntersuchung). Dazu zählen weiters Gesundheitsdaten, die von der betroffenen Person der Behörde zur Verfügung gestellt wurden (zB privatärztliche Gutachten).

„Daten über Beruf, Ausbildung und Fachkenntnisse“ der betroffenen Personen dienen in erster Linie einer zweckmäßigen Zuteilung zu einer bestimmten Waffen- und Truppengattung bzw. einer dem Ausbildungsstand entsprechenden Verwendung während des Wehrdienstes.

Personenbezogene „Daten über Einkommen, Unterhaltsverpflichtungen und Wohnsituation“ sind zB im Zusammenhang mit einem Verfahren auf Befreiung von der Leistung eines Präsenzdienstes aus besonders rücksichtswürdigen wirtschaftlichen oder familiären Interessen oder zur Ermittlung eines Anspruches auf Wohnkostenbeihilfe und/oder Familienunterhalt erforderlich.

„Militärspezifische Daten“ sind für eine zweckorientierte Einteilung und Verwendung von Soldaten beim Bundesheer zwingend erforderlich bzw. dienen als Grundlage für weitere Verwaltungstätigkeiten (zB für die Bemessung von Barbezügen).

Einzelne gesetzliche Bestimmungen sehen darüber hinaus noch weitere konkrete Verwaltungsaufgaben vor, für deren rechtmäßige Vollziehung auch die Verarbeitung personenbezogener Daten erforderlich sein kann (zB § 7 Abs. 4 betreffend die Erlaubnis zum Führen des militärischen Hoheitszeichens oder § 42 Abs. 3 betreffend die Ausstellung einer Kompetenzbilanz).

Jedenfalls sollen Datenverarbeitungen nur erfolgen dürfen, sofern es zur Wahrnehmung einer gesetzlich übertragenen Aufgabe dient und die einzelnen Daten für die Bearbeitung einer konkreten Angelegenheit tatsächlich erforderlich sind. Die diesbezüglichen einschlägigen Regelungen im Sinne des § 46 DSG wären auf Vollzugsebene durch die Verantwortlichen bzw. der von ihnen beauftragten Stellen zu treffen.

Mit der ins Auge gefassten Neutextierung des § 55a Abs. 1 und 1a werden die derzeit getrennten Regelungen des § 38 Abs. 2, § 55 Abs. 2 und § 55a Abs. 1 zusammengeführt. Dabei soll auch die bisher nur indirekt aus dem geltenden § 55a Abs. 1 Z 1 und § 38 Abs. 2 ableitbare Zulässigkeit von Datenübermittlungen innerhalb des Ressortbereiches BMLV im nunmehr vorgesehenen § 55a Abs. 1 Z 1 klarer zum Ausdruck kommen. § 38 Abs. 2 und § 55 Abs. 2 können somit entfallen. Die historisch bedingte Trennung dieser inhaltlich weitgehend identen Bestimmungen ist spätestens seit Einführung der mit BGBl. I Nr. 58/2005 geschaffenen Möglichkeit, wonach auch Wehrpflichtige einen Ausbildungsdienst leisten können, obsolet. Mit dieser beabsichtigen Maßnahme wird auch den Richtlinien 1 und 4 der Legistischen Richtlinien 1990 über die sprachliche Sparsamkeit von Rechtsvorschriften und der Vermeidung von Normwiederholungen bestmöglich entsprochen. Eine materielle Änderung ist damit nicht verbunden.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 7 und 8 (§ 60 Abs. 2p und 12):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 sind entsprechende In- und Außerkrafttretensregelungen erforderlich.

Zu Art. 118 (Änderung des Heeresdisziplinargesetzes 2014):

Zu Z 1 (§ 11 Abs. 2):

Die mit der Vollziehung des Heeresdisziplinargesetztes betrauten Behörden ergeben sich aus § 11 Abs. 1 (Disziplinarkommandanten und Disziplinarkommissionen) sowie §§ 56 und 77 (Heerespersonalamt). Hinsichtlich des Begriffes „Verarbeitung“ von Daten siehe die entsprechenden Erläuterungen zu Art. 117 Z 1 bis 6. Potentiell kommen alle in § 55a Abs. 1 WG 2001 in der vorliegenden Fassung genannten Datenarten auch für eine Verarbeitung nach dem Heeresdisziplinargesetz 2014 in Betracht (zB Gesundheitsdaten, wenn die Frage beantwortet werden soll, ob eine vorliegende Gesundheitsschädigung im Zusammenhang mit einem bestimmten Wehrdienst steht oder auf eine bereits vor dem Wehrdienst bestehende Gesundheitsschädigung zurückzuführen ist), weshalb diesbezüglich auf § 55a Abs. 1 WG 2001 verwiesen werden soll. Darüber hinaus soll durch die Zulässigkeit der Verarbeitung von „Daten über Verwaltungsstrafverfahren und Strafverfahren nach der Strafprozessordnung 1975“ auch eine allenfalls erforderliche disziplinäre Würdigung im Falle eines Zusammentreffens strafbarer Handlungen mit Pflichtverletzungen (§ 5) sichergestellt werden, zB für den Fall, dass ein (Verwaltungs)strafverfahren eingestellt wurde.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 89 Abs. 2):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 119 (Änderung des Heeresgebührengesetzes 2001):

Zu Z 1 (§ 51 Abs. 2):

Hinsichtlich des Begriffes „Verarbeitung“ von Daten siehe die entsprechenden Erläuterungen zu Art. 117 Z 1 bis 6. Potentiell kommen alle in § 55a Abs. 1 WG 2001 in der vorliegenden Fassung genannten Datenarten auch für eine Verarbeitung nach dem Heeresgebührengesetz 2001 in Betracht, weshalb diesbezüglich auf § 55a Abs. 1 WG 2001 verwiesen werden soll. Die Relevanz dieser Datenarten ergibt

sich aus dem Anwendungsbereich des Heeresgebührengesetzes 2001. So werden etwa Gesundheitsdaten für die Vollziehung des 4. Hauptstückes (Leistungen bei Erkrankung oder Verletzung) und Daten über Einkommen, Unterhaltsverpflichtungen und Wohnsituation für die Berechnung der Wohnkostenbeihilfe oder den Anspruch auf Entschädigung erforderlich sein.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 60 Abs. 2r):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 120 (Änderung des Auslandseinsatzgesetzes 2001):

Zu Z 1 (§ 6a Abs. 2 und 3):

Hinsichtlich der Ersetzung des Begriffes „Verwenden“ durch „Verarbeitung“ sowie die Auslegung des Begriffes „Verarbeitung“ von Daten siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Zu Z 2 (§ 7 Abs. 2):

Hinsichtlich des Verweises auf § 55a Abs. 1 Z 1 bis 3 und 5 („Grunddaten“, „Gesundheitsdaten“, „Daten über Ausbildung, Beruf und Fachkenntnisse“ und „Militärspezifische Daten“) siehe die entsprechenden Erläuterungen zu Art. 117 Z 1 bis 6.

Die mit der Vollziehung betrauten Behörden und die ihnen jeweils übertragenen Aufgaben ergeben sich unmittelbar aus dem Auslandseinsatzgesetz 2001 (§ 7 Abs. 1) bzw. aus den sonstigen einschlägigen wehrrechtlichen Bestimmungen, welche im Zusammenhang mit einem Auslandseinsatz anzuwenden sind (zB Teile des Heeresdisziplinargesetzes 2014). Die Verarbeitung von Gesundheitsdaten wird vor allem im Rahmen der Feststellung der Eignung zum Auslandseinsatzpräsenzdienst (§ 2 Abs. 4) erforderlich sein; Daten über Ausbildung, Beruf und Fachkenntnisse dienen in erster Linie einer zweckmäßigen Einberufung zu einem bestimmten Auslandseinsatz.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 3 (§ 11 Abs. 2k):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 121 (Änderung des Militärbefugnisgesetzes):

Zu Z 1, 5 und 10 (Inhaltsverzeichnis zu § 5a und § 5a samt Überschrift, § 26 Abs. 4 und § 31 Abs. 3):

Die in Rede stehenden Aufgaben und Befugnisse, zu deren Erfüllung die Verarbeitung personenbezogener Daten erforderlich ist, umfassen jene des 2. und 3. Teiles des Militärbefugnisgesetzes (MBG); die für den Rechtsschutz erforderlichen Datenverarbeitungen haben ihre gesetzliche Grundlage im 4. Teil des Militärbefugnisgesetzes. Hinsichtlich des Verweises auf § 55a Abs. 1 Z 1 und 3 bis 5 („Grunddaten“, „Daten über Ausbildung, Beruf und Fachkenntnisse“, „Daten über Einkommen, Unterhaltsverpflichtungen und Wohnsituation“ sowie „Militärspezifische Daten“) siehe die entsprechenden Erläuterungen zu Art. 117 Z 1 bis 6. Potentiell kommen alle diese Datenarten auch für eine Verarbeitung nach dem Militärbefugnisgesetz in Betracht, weshalb diesbezüglich auf § 55a Abs. 1 Z 1 und 3 bis 5 WG 2001 verwiesen werden soll (zB können Einkommensdaten im Rahmen der Entschädigungsbemessung nach §§ 43ff MBG benötigt werden). Einschränkungen ergeben sich auf Grund der für die Vollziehung der jeweiligen Materie festgelegten Aufgabenbereiche (zB § 6) und der Notwendigkeit der Datenverarbeitung im Einzelfall. Besondere gesetzliche Bestimmungen über die Verarbeitung von Daten bleiben davon unberührt (zB § 22).

Mit der vorgesehenen Bestimmung (§ 5a MBG) soll weiters eine für das gesamte Militärbefugnisgesetz grundlegende Regelung über die Verarbeitung personenbezogener Daten geschaffen werden. Die materiellen Inhalte der derzeit geltenden §§ 15, 26 Abs. 4 und 31 Abs. 3 lassen sich vollinhaltlich unter der nunmehr vorgesehenen Bestimmung subsumieren auf können daher ersatzlos entfallen. Mit dieser beabsichtige Maßnahme wird auch den Richtlinien 1 und 4 der Legistischen Richtlinien 1990 über die sprachliche Sparsamkeit von Rechtsvorschriften und der Vermeidung von Normwiederholungen bestmöglich entsprochen. Eine materielle Änderung ist damit nicht verbunden. Für die Verarbeitung personenbezogener Daten in militärischen Angelegenheiten, die vom Militärbefugnisgesetz nicht explizit

geregelt werden, gelten weiterhin die entsprechenden datenschutzrechtlichen Regelungen; dies betrifft insbesondere die in Betracht kommenden Löschungsbestimmungen nach dem Datenschutzgesetz.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 und 6 (Inhaltsverzeichnis zu § 15 und § 15 samt Überschrift):

Im Rahmen der mit 1. Jänner 2006 in Kraft getretenen SPG-Novelle 2006, BGBl. I Nr. 158/2005, wurde im Sicherheitspolizeigesetz (§§ 53 und 54 SPG) ausdrücklich auf „Bild- und Tonaufzeichnungsgeräte“ bei der Wahrnehmung bestimmter sicherheitspolizeilicher Aufgaben Bedacht genommen. Weiters wurde die „Videoüberwachung“ im Rahmen der DSG-Novelle 2010, BGBl. I Nr. 133/2009, (§§ 50a ff DSG 2000) explizit geregelt, „sofern nicht durch andere Gesetze Besonderes bestimmt ist“. Der am 25. Mai 2018 in Kraft tretende neue § 12 DSG („Bildverarbeitung“) wird ebenfalls nicht für entsprechende Maßnahmen zur Vollziehung hoheitlicher Aufgaben gelten; diesbezüglich wird (weiterhin) eine gesonderte gesetzliche Grundlage notwendig sein (vgl. die Erläuterungen zur RV 1664 BlgNR, XXV. GP).

Vor diesem Hintergrund soll im Abs. 1 für den „Wachdienst“ eine eigene diesbezügliche Bestimmung geschaffen werden. Neben der Echtzeitüberwachung soll auch eine kurzfristige Bildaufzeichnung zulässig sein, sofern noch ein zeitlicher Zusammenhang mit der Möglichkeit der Abwehr von Angriffen gegen militärische Rechtsgüter hergestellt werden kann. Auch in diesen Fällen sollen subsidiär die entsprechenden datenschutzrechtlichen Regelungen gelten; dies betrifft insbesondere die in Betracht kommenden Löschungsbestimmungen nach dem Datenschutzgesetz. Da Aspekte der Strafrechtspflege ohnehin nicht zu den Aufgaben des Wachdienstes gehören, sind diesbezügliche Determinierungen – insbesondere hinsichtlich eines allfälligen Abgleiches gewonnener Bilddaten zu kriminalpolizeilichen Zwecken – entbehrlich.

Der im Abs. 2 vorgesehene Hinweis auf eine Bildverarbeitung entspricht weitgehend der Intention des § 13 Abs. 5 DSG nach Transparenz und korrespondiert inhaltlich mit der Kennzeichnungspflicht betreffend „militärische Bereiche“ nach § 1 Abs. 3 MBG und kann im Einsatzfall auch Bereiche nach § 6 Abs. 3 Z 1 MBG betreffen. Als „lex specialis“ zu § 13 Abs. 5 DSG soll jedoch im Einzelfall von einem Hinweis Abstand genommen werden können. Dies wird in der Praxis jene militärischen Liegenschaften betreffen, die aus Gründen der „militärischen Sicherheit“ eine möglichst geringe Aufmerksamkeit in der Öffentlichkeit erwecken sollen. Bei der Beantwortung der Frage der „Unerlässlichkeit“ des Entfalles eines entsprechenden Hinweises wird – ebenso wie nach § 12 Abs. 2 MBG – ein strenger Maßstab anzulegen sein.

Zu Z 3, 7 und 8 (Inhaltsverzeichnis zu § 22, die Überschrift zu § 22 und § 22 Abs. 1):

Auf Grund der Tatsache, dass § 22 als „lex specialis“ zur generellen Norm des vorgesehenen § 5a (Verarbeitung personenbezogener Daten) anzusehen ist, waren sowohl die Überschrift als auch Abs. 1 entsprechend zu adaptieren. Ergänzend zu personenbezogenen Daten nach § 5a sollen militärische Organe und Dienststellen darüber hinaus auch jene unter § 39 DSG („besonderer Kategorien personenbezogener Daten“) zu subsumierenden Daten verarbeiten dürfen, sofern dies zur Erfüllung der Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr unbedingt erforderlich und verhältnismäßig im Sinne des Grundsatzes nach § 4 ist. Dabei sind angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen; eine vergleichbare Regelung ist auch im ggstl. Entwurf zu § 51 SPG vorgesehen und wird adäquat auszulegen sein. Die Definition der militärischen Organe und Dienststellen ergibt sich aus den entsprechenden Legaldefinitionen in § 1 Abs. 1 und 2. Weiters kann es in Einzelfällen, insbesondere beim Einsatz sensibler Ermittlungsmethoden, erforderlich sein, das Informationsrecht von Personen auch nach den §§ 43 Abs. 1 und 45 Abs. 4 DSG zu sistieren, um den zuständigen militärischen Organen und Dienststellen die Erfüllung ihrer gesetzlichen Aufgaben (vgl. § 20 Abs. 1 und 2) im vollem Umfang zu ermöglichen. Eine solche Sistierung wird sich jedoch vor dem Hintergrund, dass die genannten Bestimmungen nur eine allgemeine Informationspflicht vorsehen, auf spezifische, besonders gelagerte Einzelfälle zu beschränken haben. Diesfalls wird durch die dafür in Betracht kommenden Organe und Dienststellen ein besonders strenger Maßstab bei der Abwägung von Interessen der nationalen Sicherheit gegenüber der Interessen der betroffenen Person stattzufinden haben.

Zu Z 4, 11 und 12 (§ 1 Abs. 6, § 54 Abs. 4 und § 57 Abs. 6):

Hinsichtlich der Ersetzung der Begriffe „Daten“ durch den Begriff „personenbezogene Daten“ und „Verwenden“ durch „Verarbeitung“ sowie die Auslegung des Begriffes „Verarbeitung“ von Daten siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Sofern auf Bestimmungen des Datenschutzgesetz 2000 (DSG 2000) verwiesen wird, wären entsprechende Änderungen der jeweiligen Verweisung auf das Datenschutzgesetz (DSG) vorzunehmen.

Zu Z 5 (§ 5a samt Überschrift):

Siehe die Erläuterungen zu Z 1.

Zu Z 6 (§ 15 samt Überschrift):

Siehe die Erläuterungen zu Z 2.

Zu Z 7 und 8 (Überschrift zu § 22 und § 22 Abs. 1):

Siehe die Erläuterungen zu Z 3.

Zu Z 9 (§ 24 Abs. 1 und § 25 Abs. 3):

Der Diktion des DSG folgend (vgl. zB §§ 7 und 8 DSG) und in Entsprechung der Richtlinien 31 der Legistischen Richtlinien 1990 über die Einheit der Rechtssprache soll der Begriff „Zustimmung“ durch den Begriff „Einwilligung“ ersetzt werden. Materielle Änderungen sind damit nicht verbunden.

Zu Z 10 (§ 26 Abs. 4 und § 31 Abs. 3):

Siehe die Erläuterungen zu Z 1.

Zu Z 11 und 12 (§ 54 Abs. 4 und § 57 Abs. 6):

Siehe die Erläuterungen zu Z 4.

Zu Z 13 und 14 (§ 61 Abs. 1l und 3e):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 sind entsprechende In- und Außerkrafttretensregelungen erforderlich.

Zu Art. 122 (Änderung des Sperrgebietsgesetzes 2002):

Zu Z 1 (§ 1 Abs. 4):

Die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem Gesetz (§ 6a). Hinsichtlich der Begriffe „Grunddaten“ und „Verarbeitung“ von Daten siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 7 Abs. 7):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 123 (Änderung des Munitionslagergesetzes 2003):

Zu Z 1 (§ 1 Abs. 3):

Die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem Gesetz (§ 14). Hinsichtlich der Begriffe „Grunddaten“ und „Verarbeitung“ von Daten siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 18 Abs. 7):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 124 (Änderung des Militärauszeichnungsgesetzes 2002):

Zu Z 1 (§ 3 Abs. 4):

Die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem Gesetz (zB § 6, § 8b oder § 9 Abs. 3 bis 5). Hinsichtlich der Begriffe „Verarbeitung“ von Daten, „Grunddaten“ und „Militärspezifische Daten“ siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 18 Abs. 4f):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 125 (Änderung des Verwundetenmedaillengesetzes):

Zu Z 1 (§ 4 Abs. 2a):

Die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem Gesetz. Hinsichtlich der Begriffe „Verarbeitung“ von Daten, „Grunddaten“ und „Gesundheitsdaten“ siehe die Erläuterungen zu Art. 117 Z 1 bis 6.

Zur Stellung des Bundesministers und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 6a Abs. 5):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zu Art. 126 (Änderung des Truppenaufenthaltsgesetzes):

Zu Z 1 (§ 5a samt Überschrift):

Die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden ergeben sich unmittelbar aus dem Gesetz (§ 2). Hinsichtlich der Begriffe „Verarbeitung“ von Daten und „Grunddaten“ siehe die Erläuterungen zu Art. 117 Z 1 bis 6. Darüber hinaus sollen völkerrechtlicher Vereinbarungen speziellere Datenschutzregelungen vorsehen können (Abs. 2).

Zur Stellung des Bundesministers für Landesverteidigung und der sonstigen Behörden als Verantwortliche siehe die Erläuterungen zu „Allgemeines“.

Zu Z 2 (§ 7 Abs. 3):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Zum 10. Hauptstück (Landwirtschaft und Umwelt)

Zu Art. 127 (Änderung des Abfallwirtschaftsgesetzes 2002)

Allgemeines:

Anpassungen an die neuen datenschutzrechtlichen Vorgaben, insbesondere an die Datenschutz-Grundverordnung (DSGVO), sind auch im Abfallwirtschaftsgesetz 2002 (AWG 2002), BGBl. I Nr. 102/2002, erforderlich.

Die im AWG 2002 geregelten Datenverarbeitungen, insbesondere die elektronischen Register, müssen ab dem 25. Mai 2018 den durch die DSGVO geänderten Anforderungen genügen, zumal darin unter anderem auch personenbezogene Daten natürlicher Personen verarbeitet werden.

Die gemäß § 22 AWG 2002 eingerichteten elektronischen Register stehen im Einklang mit den e-Governmentvorgaben (insb. Effizienzsteigerung, serviceorientierte Verwaltung, One-Stop-Shop- und Once-Only-Prinzip), dem EU eGovernment Action Plan 2016-2020 und der EU-E-Government Ministererklärung von Tallinn und stellen einen bedeutenden Strategiebereich zur Digitalisierung von Verwaltungsvorgängen im Umweltrecht dar. Zur Anpassung der diesbezüglich bestehenden Bestimmungen an die neuen datenschutzrechtlichen Vorgaben sind im Wesentlichen formal-redaktionelle Überarbeitungen notwendig.

Vor dem Hintergrund, dass im neuen Datenschutzrecht weder der Begriff des „Informationsverbundsystems“ noch der Begriff „Betreiber“ existiert, erfolgen Anpassungen entsprechend der DSGVO.

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 12 B-VG („Abfallwirtschaft“).

Zu Art. 127 Z 1 (§ 21 Abs. 2c AWG 2002):

Anpassung der Begrifflichkeiten („verarbeiten“ statt „verwenden“). Wie bisher ist die BMNT mit dieser Bestimmung ermächtigt, auch Daten von Nicht-Registrierungspflichtigen von Amts wegen im Stammdatenregister gemäß § 22 Abs. 1 Z 1 zu erfassen bzw. in den jeweiligen Bewegungsdatenregistern gem. § 22 Abs. 1 Z 2 lit. a bis d zu verarbeiten. Die Anpassung der Begrifflichkeiten macht es sprachlich notwendig, diese Regelung noch präziser auszuführen und auch auf die Verarbeitung der Daten in den Registern gem. § 22 Abs. 1 Z 2 lit. a bis d („Bewegungsdatenregister“) Bezug zu nehmen.

Zu Art. 127 Z 2 (§ 22 Abs. 2 AWG 2002):

Anpassung der Begrifflichkeiten („verarbeiten“ statt „verwenden“). Die Anpassung der Begrifflichkeiten macht es sprachlich notwendig, diese Regelung noch präziser auszuführen und neben der Verarbeitung im Stammdatenregister gem. § 22 Abs. 1 Z 1 auch auf die Verarbeitung der Daten in den Registern gem. § 22 Abs. 1 Z 2 lit. a bis d („Bewegungsdatenregister“) Bezug zu nehmen.

Zu Art. 127 Z 3 (§ 22 Abs. 4 bis 5c AWG 2002):

Im Hinblick auf die Tatsache, dass sowohl die BMNT als auch die Landeshauptleute im Rahmen ihrer Zuständigkeit über einzelne Datenverarbeitungen entscheiden und daran maßgeblich beteiligt sind, erfolgt die Klarstellung, dass es sich hier um „gemeinsam für die Verarbeitung Verantwortliche“ im Sinne des Art. 26 DSGVO handelt.

Schon bisher ist die BMNT als Betreiberin der Register festgelegt. Wie bisher kommt die Aufgabe, erforderlichenfalls technische Maßnahmen im Rahmen des Betriebs, der Wartung und der Weiterentwicklung der Register gegenüber Auftragsverarbeitern zu beauftragen, der BMNT zu.

Wie bisher erfolgen die Zugriffe auf Daten der Register durch die zuständigen Mitarbeiterinnen und Mitarbeiter der zuständigen Behörden nach einem Rollen- und Rechtekonzept, das den eGovernment-Vorgaben Rechnung trägt. Die Zwecke der Datenverarbeitung sowie die zu verarbeitenden Daten ergeben sich aus den bestehenden Bestimmungen des AWG 2002, insb. aus § 22 Abs. 1 und Abs. 5 ff, §§ 86, 87 und 87a AWG 2002. Die verarbeiteten Daten sind in § 22 und § 22a genannt und werden – soweit erforderlich – auch in den jeweiligen Verordnungen, zB gemäß §§ 14 und 23 AWG 2002, präzisiert.

Zu Abs. 5 bis 5c AWG 2002: Anpassung der Begrifflichkeiten sowie Anpassungen an das Bundesministeriengesetz idgF. Angelegenheiten des Bergwesens ist nunmehr im Wirkungsbereich der BMNT gelegen. Wie bisher dürfen die Daten der Register als eGovernmentsystem auch von anderen Bundesministerinnen und Bundesministern sowie den zuständigen Behörden verarbeitet werden. Soweit eine Verarbeitung durch andere Bundesministerinnen und Bundesminister als die BMNT erfolgt, sind auch diese Verantwortliche im Sinne des Art. 4 DSGVO (zB Verpflichtung zur Berücksichtigung der Datenverarbeitung im Verzeichnis aller Verarbeitungstätigkeiten gem. Art. 30 DSGVO).

Im Hinblick auf die Möglichkeit der Nutzung der IT-technischen Infrastruktur der Register durch die jeweiligen Landesregierungen (Abs. 5d) ist anzumerken, dass diese gegebenenfalls ebenfalls bei der Datenverarbeitung personenbezogener Daten als Verantwortliche im Sinne der DSGVO agieren.

Zu Art. 127 Z 4 (§ 22 Abs. 6 AWG 2002):

Anpassung der Begrifflichkeiten.

Zu Art. 127 Z 5 (§ 22 Abs. 8 bis 10 AWG 2002):

Registrierungspflichtige sind dazu verpflichtet, die Daten der Register aktuell zu halten und können diese im Regelfall selbst ändern bzw. berichtigen (§ 22b) und selbst abfragen. Für den Fall, dass eine betroffene Person ihre Daten nicht ändern bzw. berichtigen kann, hat die zuständige Behörde als Verantwortliche die Pflichten gemäß der DSGVO vorzunehmen. Im Hinblick darauf, dass die zuständige Behörde und die BMNT als gemeinsam für die Verarbeitung Verantwortliche zu qualifizieren sind und die Stammdaten entsprechend dem Once-Only-Prinzip für mehrere „Zwecke“ bzw. Meldungen zur Verfügung stehen, erfolgt bei Eingriffen in die Stammdaten eine Abstimmung zwischen der zuständigen Behörde und der BMNT. Daher wird die BMNT für bestimmte Stamm- und Bewegungsdaten als datenschutzrechtliche Anlaufstelle für die betroffene Person festgelegt, an die sich die betroffene Person zu wenden hat bzw. an die die betroffene Person zu verweisen ist. Dies gilt nicht, wenn es sich bei den erfassten Daten um Erlaubnisse oder Genehmigungen, sohin um Daten gemäß § 22a Abs. 1 lit. a, b oder c, Abs. 3a und Abs. 4 AWG 2002 handelt. In diesen Fällen hat sich die betroffene Person direkt an die jeweils zuständige Behörde (Landeshauptleute) zu wenden.

Im Register werden Meldungen erfasst und nachvollziehbar dokumentiert. Dateninhalte einer Meldung müssen zum Zeitpunkt des Einbringens der Meldung für Kontrollaufgaben der Behörde zur Verfügung stehen. Eine nachträgliche Änderung von an die Behörde übermittelten Meldungen würde dem

Dokumentationszweck der Register zuwiderlaufen und hat daher im Hinblick auf die Wahrnehmung behördlicher Kontrollaufgaben zu unterbleiben. Allerdings kann eine Meldung vom Meldepflichtigen insoweit ohnehin berichtigt, aktualisiert und vervollständigt werden, als dieser eine korrigierte Meldung einbringen kann.

Zudem sind gemäß Art. 5 Abs. 1 lit. d DSGVO nur solche personenbezogenen Daten unverzüglich zu löschen oder zu berichtigen, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind.

Klargestellt wird, dass die Bundesministerin für Nachhaltigkeit und Tourismus die Daten der Register auch zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken verarbeiten darf. Diese Verarbeitung unterliegt den Bestimmungen der DSGVO. Die Bedingungen und Garantien gemäß Art. 89 DSGVO sind sicherzustellen, insbesondere durch Verarbeitung nur jener Daten, die für den jeweiligen Zweck angemessen, erheblich und notwendig sind (Datenminimierung). Auch bei einer Verarbeitung zu den oben genannten Zwecken ist jedenfalls Folgendes sicherzustellen: Einhaltung des Rollen- und Rechtskonzepts des EDM mit eingeschränkten Zugriffen und mit Benutzerverwaltung durch das BMNT, Datenschutzschulung, das Löschen von Zwischenergebnissen und Hilfsdokumenten, die für den Zweck der Verarbeitung nicht mehr benötigt werden, Anforderungen an die Sicherheit der verwendeten Endgeräte und Sicherheitsüberprüfungen nach dem Stand der Technik.

Zu Art. 127 Z 6 (§ 22b Abs. 4 AWG 2002):

Um sicherzustellen, dass die in den Registern erfassten Stammdaten im Sinne des Artikel 5 der DSGVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind, dürfen auch die zuständigen Behörden als Hilfestellung für den Registrierungspflichtigen Datenanpassungen vornehmen. Zudem kann eine Stammdatenergänzung erforderlich sein, um die Erfassung von Genehmigungsinhalten von Anlagen durch die Behörde zu ermöglichen oder das Unternehmen bei der Erfüllung von Meldepflichten zu unterstützen. Diese Ermächtigung entbindet den jeweiligen Registrierungspflichtigen nicht von seinen Verpflichtungen gemäß § 22b Abs. 1.

Die registrierungspflichtige Person ist von Änderungen an den Stammdaten zu verständigen, wenn diese Auswirkungen auf die Einhaltung von Melde- oder Betreiberpflichten haben. Die Verständigung hat insbesondere mittels der in den Registern vorhandenen Werkzeuge (EBB) oder allenfalls auch mittels Nachricht an die erfasste Kontakt-E-Mail-Adresse zu erfolgen.

Keine Verständigung ist zB bei reinen Neugliederungen der Stammdaten zur besseren Übersichtlichkeit erforderlich oder damit der Behörde ermöglicht wird, Genehmigungsinhalte gezielt zu erfassen.

Zu Art. 128 (Änderung des Weingesetzes 2009)

Allgemeines:

Mit der vorliegenden Novelle zum Weingesetz 2009 erfolgt die Umsetzung der Datenschutz-Grundverordnung im Weinbereich. Diese Verordnung ist am 25. Mai 2016 in Kraft getreten, kommt ab 25. Mai 2018 zur Anwendung und hebt die zu diesem Zeitpunkt die Richtlinie 95/46/EG auf.

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich insofern auf Art. 10 Abs. 1 Z 12 B-VG („Ernährungswesen“).

Zu Art. 128 Z 1 (§ 26a samt Überschrift):

§ 26a legt insbesondere die gemeinsamen Verantwortlichen und Auftragsverarbeiter sowie deren Rechte und Pflichten fest.

Zu Abs. 1:

Der DSGVO ist der bisher vorgesehene Begriff des Informationsverbundsystems unbekannt. Art. 26 dieser Verordnung spricht von „gemeinsam Verantwortlichen“, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.

Gemeinsam Verantwortliche sind das Bundesministerium für Nachhaltigkeit und Tourismus, die Höhere Bundeslehranstalt und Bundesamt für Wein- und Obstbau in Klosterneuburg, das Bundesamt für Weinbau in Eisenstadt, die Bundeskellereiinspektion, sowie die betroffenen Landesbehörden.

Diese Behörden sind ermächtigt, die im Weinbereich ermittelten Daten (z. B. betreffend die Ernte- oder Bestandsmeldungen) zur Führung der Weindatenbank im Bundesministerium für Nachhaltigkeit und Tourismus gemeinsam zu verarbeiten.

Zu Abs. 2:

Es wird ausdrücklich festgelegt, dass die Erfüllung von in der DSGVO festgelegten Pflichten (z. B. Informationspflichten) jedem Verantwortlichen obliegt, der konkret für das jeweilige Verfahren und die Verarbeitung der Daten zuständig ist bzw. war. Wendet sich ein Betroffener an einen unzuständigen Verantwortlichen, so ist Ersterer an den zuständigen Verantwortlichen zu verweisen.

Zu Abs. 3:

Abs. 3 des neuen § 26a regelt die „Auftragsverarbeiter“. Diese Funktion üben die Gemeinden und beauftragten Unternehmen gemäß § 24 des Weingesetzes 2009 aus (gemäß Art. 4 Z 8 iVm Art. 28 Abs. 1 DSGVO). Auch die Auftragsverarbeiter werden ausdrücklich verpflichtet, die in der DSGVO festgelegten Datenschutzpflichten wahrzunehmen. Sie haben insbesondere auch datenqualitätssichernde Maßnahmen zu setzen.

Zu Abs. 4:

Die Auftragsverarbeiter gemäß Abs. 3 haben gemeinsam mit dem jeweiligen Verantwortlichen die Rechtmäßigkeit der Verarbeitung der Daten in Hinblick auf die Vollziehung des Weingesetzes 2009 zu überprüfen.

Zu Abs. 5:

Festgelegt wird die Pflicht, die Daten über die durchgeführten Verarbeitungsvorgänge drei Jahre lang aufzubewahren.

Zu Z 2 (§ 74 Abs. 6):

Auf Grund des Inkrafttretens des Datenschutzgesetzes mit 25. Mai 2018 ist eine entsprechende Inkrafttretensregelung erforderlich.

Anlage

Zum 2. Abschnitt (Öffentlicher Dienst)

DATENSCHUTZ-FOLGENABSCHÄTZUNG

SYSTEMATISCHE BESCHREIBUNG

der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen

Im 5a. Unterabschnitt des Beamten-Dienstrechtsgesetzes 1979 – BDG 1979, BGBl. Nr. 333/1979, wird die Nutzung der Informations- und Kommunikationstechnologie oder -technik (IKT) geregelt, die insbesondere die Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit (vgl. § 79f BDG 1979), die Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung (vgl. § 79g BDG 1979) sowie sonstige zulässige Datenverarbeitungen (vgl. § 79h BDG 1979) umfasst.

§ 204 Abs. 7 BDG 1979, § 3 Abs. 4 Vertragsbedienstetengesetz 1948 – VBG, BGBl. Nr. 86/1948, § 3 Abs. 1 Richter- und Staatsanwaltschaftsdienstgesetz – RStDG, BGBl. Nr. 305/1961, § 6 Abs. 5 Landeslehrer-Dienstrechtsgesetz – LDG 1984, BGBl. Nr. 302/1984, § 6 Abs. 5 Land- und forstwirtschaftliches Landeslehrer-Dienstrechtsgesetz – LLDG 1985, BGBl. Nr. 296/1985, und § 2 Abs. 3a Rechtspraktikantengesetz – RPG, BGBl. Nr. 644/1987, regeln die Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten durch die jeweilige Dienstbehörde oder Personalstelle. Neben der Prüfung etwaiger Zulassungserfordernisse sind vor allem die Einholung und Verarbeitung von Strafregistereinkünften gemäß den §§ 9 und 9a des Strafregistergesetzes 1968, BGBl. Nr. 277/1968, sowie die Abfrage und Verarbeitung von Vorwarnungen nach Art. 56a der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen, ABl. Nr. L 255 vom 30.09.2005 S. 22, zuletzt geändert durch den Delegierten Beschluss (EU) 2017/2113, ABl. Nr. L 317 vom 01.12.2017 S. 119, im Binnenmarkt-Informationssystem (IMI) vorgesehen.

Die Leiterinnen und Leiter der Zentralstellen sind ermächtigt, personenbezogene Daten und besondere Kategorien personenbezogener Daten der Personen gemäß § 280 Abs. 1 BDG 1979 im Sinne des Art. 4 Z 2 der Datenschutz-Grundverordnung zu verarbeiten, einander zu übermitteln (Übermittlung) und zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zu verarbeiten (Weiterverarbeitung). Eine solche Verarbeitung, Übermittlung oder Weiterverarbeitung muss entweder zum Zwecke der Aufrechterhaltung oder des Funktionierens der Administration des öffentlichen Dienstes, oder zum Zwecke der Erfüllung der rechtlichen Verpflichtungen oder der Geltendmachung der Rechte, die sich aus den in § 280 Abs. 2 Z 2 BDG 1979 genannten Vorschriften ergeben, oder gemäß § 280 Abs. 2 Z 3 BDG 1979 zum Zwecke der Ausübung der in den Vorschriften gemäß § 280 Abs. 2 Z 2 BDG 1979 übertragenen öffentlichen Gewalt erforderlich sein. Eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung oder Weiterverarbeitung ist, sofern nicht ausdrücklich normiert, gemäß § 280 Abs. 1 und 2 BDG 1979 nicht vorgesehen.

§ 280 Abs. 3 BDG 1979 ermächtigt die Leiterinnen und Leiter der Zentralstellen, personenbezogene Daten und besondere Kategorien personenbezogener Daten gemäß § 280 Abs. 1 BDG 1979 auf Ersuchen einer zuständigen Behörde gemäß § 36 Abs. 2 Z 7 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, deren Aufgabe die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, die Strafvollstreckung oder der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit ist, unter den im Gesetz angeführten Voraussetzungen zu verarbeiten.

§ 280 Abs. 5 BDG 1979 ermächtigt die Bundesministerin oder den Bundesminister für öffentlichen Dienst und Sport, soweit dies zum Zwecke der Wahrnehmung der ihr oder ihm in Vollziehung dieses Bundesgesetzes oder anderer in § 280 Abs. 2 Z 2 BDG 1979 genannter Vorschriften übertragenen Mitwirkungsbefugnisse erforderlich ist, in die von § 280 Abs. 1 BDG 1979 erfassten Datenverarbeitungssysteme direkt Einsicht zu nehmen und im Einzelfall erforderlichenfalls nicht inhaltsändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen zum Zwecke der Sicherung der Datenqualität vorzunehmen.

§ 280 Abs. 6 BDG 1979 ermächtigt die Bundesministerin oder den Bundesminister für öffentlichen Dienst und Sport, personenbezogene Daten und besondere Kategorien personenbezogener Daten aus von § 280 Abs. 1 BDG 1979 erfassten Datenverarbeitungssystemen zu statistischen Auswertungen und zu wissenschaftlichen oder historischen Forschungszwecken unter den angeführten Voraussetzungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten. Soweit hiebei besondere Kategorien personenbezogener Daten verarbeitet werden, muss ein schriftlich zu dokumentierendes wichtiges öffentliches Interesse an der Untersuchung vorliegen. Erforderlichenfalls ist die Bundesministerin oder

der Bundesminister für öffentlichen Dienst und Sport ermächtigt, im Einzelfall nicht inhaltsändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen der genannten Daten zum Zwecke der Sicherung der Datenqualität vorzunehmen.

Gemäß § 280 Abs. 7 BDG 1979 ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport ermächtigt, unter den angeführten Voraussetzungen erforderlichenfalls aus den von § 280 Abs. 1 BDG 1979 erfassten Datenverarbeitungssystemen Adressdaten für Benachrichtigungen oder Befragungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten.

§ 280a Abs. 1 BDG 1979 sieht zum Zwecke der eindeutigen Identifikation im Beschäftigungskontext die Möglichkeit der elektronischen Personenkennzeichnung der in § 280 Abs. 1 BDG 1979 angeführten Personen vor. Dies kann durch eine aus der ZMR-Zahl (§ 16 Abs. 4 des Meldegesetzes 1991, BGBl. Nr. 9/1992) durch bereichsspezifische Verschlüsselung abgeleitete Personenkennzeichnung oder durch ein bereichsspezifisches Personenkennzeichen (bPK) gemäß § 9 des E-Government-Gesetzes – E-GovG, BGBl. I Nr. 10/2004 erfolgen.

Zur Erfüllung der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 BDG 1979 sind die jeweiligen Verantwortlichen gemäß § 280a Abs. 6 BDG 1979 ermächtigt, im Zentralen Personenstandsregister Abfragen der eingetragenen Todesfälle und Todeserklärungen durchzuführen.

§ 280a Abs. 7 BDG 1979 ermächtigt die Bundeskanzlerin oder den Bundeskanzler, zum Zwecke der rechtskonformen Verfahrensgestaltung, der Fehlerbehebung sowie der Datensicherheit in den von ihr oder ihm bereitgestellten oder betriebenen IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes erforderliche nicht inhaltsändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten durchzuführen.

§ 119a LDG 1984 ermächtigt die landesgesetzlich zuständigen Behörden, personenbezogene Daten und besondere Kategorien personenbezogener Daten gemäß § 119a Abs. 1 LDG 1984 im Sinne des Art. 4 Z 2 DSGVO zu verarbeiten, einander zu übermitteln (Übermittlung) und zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zu verarbeiten (Weiterverarbeitung). Bestimmungen der §§ 280 ff BDG 1979 finden im in § 119a Abs. 2 LDG 1984 beschriebenen Umfang sinngemäß Anwendung.

§ 119h LLDG 1985 ermächtigt die landesgesetzlich zuständigen Behörden, personenbezogene Daten und besondere Kategorien personenbezogener Daten gemäß § 119h Abs. 1 LLDG 1985 im Sinne des Art. 4 Z 2 DSGVO zu verarbeiten, einander zu übermitteln (Übermittlung) und zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zu verarbeiten (Weiterverarbeitung). Bestimmungen der §§ 280 ff BDG 1979 finden im in § 119h Abs. 2 LLDG 1985 beschriebenen Umfang sinngemäß Anwendung.

§ 1a Abs. 1 bis 3, § 101 Abs. 1 und 2, § 102 und § 105 Abs. 5 Pensionsgesetz 1965 – PG 1965, BGBl. Nr. 340/1965, § 1a Abs. 1 bis 3, § 21 Abs. 1 und 2 und § 21a Abs. 1 bis 3 Bundestheaterpensionsgesetz – BThPG, BGBl. Nr. 159/1958, und § 1a Abs. 1 bis 3, § 68 Abs. 1 und 2 und § 69 Bundesbahn-Pensionsgesetz – BB-PG, BGBl. I Nr. 86/2001, ermächtigen die zuständigen Stellen, personenbezogene Daten und besondere Kategorien personenbezogener Daten zum Zwecke der Ermittlung der Pensionshöhen zu erheben und zu verarbeiten.

BEWERTUNG

der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Die Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit und auch die Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung muss dem jeweils Verantwortlichen jedenfalls möglich sein, um den ihm auferlegten Pflichten nachkommen und die ihm gewährten Rechte ausüben zu können. Dass hierbei auch besondere Kategorien personenbezogener Daten im Falle der unbedingten Erforderlichkeit verarbeitet werden können, wird insbesondere auch im Hinblick auf die durch die geltende IKT-Nutzungsverordnung ermöglichte private IKT-Nutzung einer Beamtin oder eines Beamten vorgesehen. Die Verarbeitung besonderer Kategorien personenbezogener Daten zu Kontrollzwecken wird auf Art. 9 Abs. 2 lit. b und g DSGVO gestützt. Unbedingt erforderlich ist eine Verarbeitung zu Kontrollzwecken dann, wenn mit der Verarbeitung personenbezogener Daten alleine nicht das Auslangen gefunden werden kann, um Schäden an der IKT-Infrastruktur abzuwehren, ihre korrekte Funktionsfähigkeit zu gewährleisten oder um einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung nachzugehen.

Aus dienstrechtlichen Vorschriften folgt die Notwendigkeit zur Prüfung etwaiger Zulassungserfordernisse sowie zur Einholung und Verarbeitung von Strafregistereinkünften gemäß den §§ 9 und 9a des Strafregistergesetzes 1968 sowie die Abfrage und Verarbeitung von Vorwarnungen nach Art. 56a der

Richtlinie 2005/36/EG im Binnenmarkt-Informationssystem (IMI) gemäß 204 Abs. 7 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG.

Die Notwendigkeit der Verarbeitung, Übermittlung oder Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten ergibt sich für § 280 BDG 1979 aus dem jeweiligen in § 280 Abs. 1 BDG 1979 angeführten Rechtsverhältnis im Zusammenhang mit dem jeweiligen Zweck. Für die Praxis bedeutet dies, dass beispielsweise die zum Zwecke der Auszahlung gebührender Bezüge oder Pensionen erforderlichen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten verarbeitet, übermittelt und weiterverarbeitet werden dürfen, um dieser rechtlichen Verpflichtung, die sich in diesem Fall aus einer Vorschrift gemäß § 280 Abs. 2 Z 2 BDG 1979 ergibt, nachzukommen.

Weiters ergibt sich die Notwendigkeit der beschriebenen Verarbeitungs-, Übermittlungs- und Weiterverarbeitungsvorgänge ebenfalls aus dem wichtigen öffentlichen Interesse an der Erfüllung der Kernaufgaben des Staates, an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des öffentlichen Dienstes und an einem rechtskonformen Vollzug insbesondere der in § 280 Abs. 2 BDG 1979 genannten Vorschriften, der beispielsweise ohne eine zeit- und ortsunabhängige Verfügbarkeit der jeweiligen Daten in der jetzigen Form nicht möglich wäre. Auch die Regelung der Nutzung der IKT-Infrastruktur zur Gewährleistung ihrer korrekten Funktionsfähigkeit sowie entsprechende Kontrollmöglichkeiten sind in diesem Zusammenhang in verhältnismäßigem Umfang notwendig und sachgerecht und bedingen in gewissem Ausmaß die Verarbeitung personenbezogener Daten oder besonderer Kategorien personenbezogener Daten.

Im Zusammenhang mit der Verarbeitung, Übermittlung und Weiterverarbeitung besonderer Kategorien personenbezogener Daten darf insbesondere auf Art. 9 Abs. 2 lit. b, g, h und j DSGVO verwiesen werden. Bezüglich Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit Art. 9 Abs. 3 DSGVO wird auf die Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten verwiesen (vgl. Art. 20 B-VG, § 46 BDG 1979, § 25 Abs. 6 Bundes-Gleichbehandlungsgesetz – B-GlBG, BGBl. Nr. 100/1993, § 54 Ärztegesetz 1998 – ÄrzteG 1998, BGBl. I Nr. 169/1998, …).

Bezüglich der Notwendigkeit von § 119a LDG 1984 und 119h LLDG 1985 wird auf die Ausführungen zu den §§ 280 ff BDG 1979 verwiesen.

An den Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 3 und 5 bis 7 BDG 1979 sowie § 280a Abs. 1, 6 und 7 BDG 1979 besteht ein allgemeines wichtiges öffentliches Interesse aufgrund der der oder dem Ermächtigten zukommenden Funktion in Zusammenschau mit den angeführten Zwecken.

Die Notwendigkeit zur Erhebung und Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten gemäß § 1a Abs. 1 bis 3, § 101 Abs. 1 und 2, § 102 und § 105 Abs. 5 PG 1965, § 1a Abs. 1 bis 3, § 21 Abs. 1 und 2 und § 21a Abs. 1 bis 3 BThPG sowie § 1a Abs. 1 bis 3, § 68 Abs. 1 und 2 und § 69 BB-PG ergibt sich aus pensionsrechtlichen Vorschriften.

Die Verarbeitung, Übermittlung und Weiterverarbeitung der jeweiligen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten liegt aber auch im Interesse der betroffenen Personen und ist erforderlich, damit die Verantwortlichen oder die betroffenen Personen ihre Rechte und Pflichten ausüben oder geltend machen können.

Grundsätzlich bestehen Risiken, allerdings ist deren Eintritt einerseits nicht sehr wahrscheinlich und sind andererseits zahlreiche, wirksame und auf den jeweiligen Einzelfall bezogene Abhilfemaßnahmen vorgesehen, sodass die Datenschutz-Folgenabschätzung klar positiv ausfällt.

RISIKEN

Risiken, die bei der Verarbeitung und Übermittlung von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten bestehen, werden vor allem durch die strikte Einhaltung der Erfassungs- und Bearbeitungsvorgaben (z. B. Handbücher, Sicherheitskonzepte, Verfahrensvorschriften,…) – insbesondere in den diversen Anwenderapplikationen des Personalverfahrens und der Personalabrechnungen, bei der Pensionsbemessung und Pensionsauszahlung sowie beim Personalvollzug ohne IT-Unterstützung – minimiert. Eine solche Minimierung der Risiken erfolgt standardmäßig in den IKT-Lösungen und IT-Verfahren für das IT-Personalmanagement des Bundes.

Als Risiken werden insbesondere in Erwägungsgrund 85 der DSGVO unter anderem genannt:

– „*physische, materielle oder immaterielle Schäden*“, „*unbefugte Aufhebung der Pseudonymisierung*“, „*Rufschädigung*“, „*Identitätsdiebstahl oder -betrug*“, „*finanzielle Verluste*“, „*Verlust der Vertraulichkeit bei Berufsgeheimnissen*“ oder „*erhebliche wirtschaftliche oder gesellschaftliche Nachteile*“:

Diese Risiken beziehungsweise Nachteile sind nahezu ausgeschlossen, weil mit den Strafbestimmungen des vierten bis sechsten sowie zweiundzwanzigsten Abschnittes des Besonderen Teiles des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, sowie den allenfalls anzuwendenden dienstrechtlichen Bestimmungen, wie beispielsweise dem Disziplinarrecht, wirksame Vorkehrungen gegen die unrechtmäßige Verarbeitung von Daten und somit das Entstehen von physischen, materiellen oder immateriellen Schäden bestehen. Wer die jeweiligen Daten missbraucht, geht angesichts der gerichtlichen Strafdrohung selbst ein sehr hohes Risiko ein.

Auf die Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten darf verwiesen werden (vgl. Art. 20 B-VG, § 46 BDG 1979, § 26 Bundes-Personalvertretungsgesetz, BGBl. Nr. 133/1967, § 25 Abs. 6 B-GlBG…). Insbesondere finanzielle Verluste sind trotz der Verwendung von Finanzdaten aufgrund der durchgehenden Protokollierung von Verarbeitungen, Übermittlungen und Weiterverarbeitungen und der Kontrollmöglichkeit der Daten durch die betroffenen Personen nicht zu erwarten.

Eine unbefugte Aufhebung einer Pseudonymisierung ist bei schon jetzt umgesetzten Rollenkonzepten ausgeschlossen.

– „*Verlust der Kontrolle über personenbezogene Daten*“:

Dieses Risiko wird dadurch verringert, dass Art. 5 Abs. 2 DSGVO als unmittelbar anwendbaren Grundsatz die Rechenschaftspflicht vorsieht. Die oder der Verantwortliche ist also nicht nur für die Einhaltung des Art. 5 Abs. 1 DSGVO verantwortlich, sondern muss auch dessen Einhaltung nachweisen können, was durch entsprechende Protokollierung (vgl. § 79e Abs. 2a, § 79f Abs. 5 und § 280a Abs. 4, 5 und 7 BDG 1979, § 119a LDG 1984 und § 119h LLDG 1985), Dokumentation (vgl. § 79e Abs. 2a, § 79f Abs. 3, § 204 Abs. 8, § 280 Abs. 3 und 6 und § 280b Abs. 4 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 und § 119a Abs. 2 LDG 1984, § 6 Abs. 5 und § 119h Abs. 2 LLDG 1985 und § 2 Abs. 3a RPG) und Aufbewahrungspflichten (vgl. § 280a Abs. 2 bis 5 und 7 BDG 1979, § 119a Abs. 2 LDG 1984 und § 119h Abs. 2 LLDG 1985) beziehungsweise Löschpflichten (vgl. § 204 Abs. 8 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG) erfolgt. Im PM-SAP beispielsweise besteht auch derzeit bereits ein zentrales Protokollierungssystem, das jede Verarbeitung der Daten lückenlos protokolliert beziehungsweise durch ein definiertes Rollenkonzept nicht jede Person die Daten verarbeiten lässt.

Beispiele für Regelungen, die insbesondere aus Gründen der Nachvollziehbarkeit das Schriftlichkeitserfordernis vorsehen, sind etwa § 79e Abs. 2a, § 79f Abs. 3, § 79g Abs. 1, 4, 6 und 7, § 204 Abs. 7, § 280 Abs. 3 und 6 und § 280b Abs. 4 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 und § 119a Abs. 2 LDG 1984, § 6 Abs. 5 und § 119h Abs. 2 LLDG 1985 und § 2 Abs. 3a RPG.

– „*Diskriminierung*“:

Dieses Risiko ist durch diverse Diskriminierungsverbote ausgeschlossen, insbesondere durch solche des B-GlBG oder etwa durch § 43a BDG 1979. Außerdem besteht für die betroffenen Personen in vielen Fällen die Ausübung des Rechtes auf Einsicht mittels ESS, wodurch zusätzlich eine Diskriminierung ausgeschlossen ist.

– „*Einschränkung der Rechte der betroffenen Personen*“:

Die Beschränkung der Rechte der betroffenen Person gemäß Art. 23 DSGVO erfolgt in § 280 Abs. 3 BDG 1979 im Rahmen einer Einzelfallprüfung, liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gewährleistet ist. Die zuständige Behörde soll durch die Vornahme der erforderlichen bloßen Verarbeitung durch die Leiterin oder den Leiter der jeweiligen Zentralstelle unterstützt werden. Im Einzelfall ist zu prüfen, in welchem Ausmaß die Rechte der betroffenen Person gemäß Art. 12 bis 14 und Art. 16 bis 22 DSGVO in der Zeit vom Einlangen des Ersuchens bis zum Zeitpunkt der Information der betroffenen Person beschränkt werden müssen, damit die Verwirklichung der Zwecke des Ersuchens nicht unmöglich gemacht oder ernsthaft beeinträchtigt wird. Dabei kommen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zur Anwendung. Da die entsprechenden Beschränkungen der Rechte der betroffenen Person bereits in § 280 Abs. 3 BDG 1979 kundgemacht werden und eine Unterrichtung über die Beschränkung im Einzelfall dem Zwecke der Beschränkung abträglich wäre, ist ein Informieren der betroffenen Person erst vorgesehen, sobald es nicht mehr dem Zweck des Ersuchens zuwiderläuft oder zuwiderlaufen kann. Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung ergeben sich aus den jeweiligen Verfahrensrechten. Für den Bereich des § 280 Abs. 3 BDG 1979, also der bloßen Verarbeitung aufgrund eines entsprechenden Ersuchens, ist die Leiterin oder der Leiter der jeweiligen Zentralstelle Verantwortlicher. Die Speicherfristen richten sich

nach § 280a Abs. 2 bis 5 BDG 1979 oder nach den gemäß § 280 Abs. 7 BDG 1979 erlassenen Verordnungen. Das Informieren der betroffenen Person gemäß Art. 12 bis 14 DSGVO hat erst nach Mitteilung durch die ersuchende zuständige Behörde an die Leiterin oder den Leiter der jeweiligen Zentralstelle direkt zu erfolgen, was bedeutet, dass es zu keiner Befassung von Zwischenvorgesetzten kommen soll. Zudem wird der betroffenen Person ein Recht zur Stellungnahme gegenüber der Leiterin oder dem Leiter der Dienststelle eingeräumt. § 280 Abs. 3 BDG 1979 regelt ausschließlich die bloße Verarbeitung aufgrund eines Ersuchens zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, der Strafvollstreckung oder des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Sonstige Ersuchen sind gemäß § 280 Abs. 1 und 2 BDG 1979 oder gemäß ihrer jeweiligen Rechtsgrundlage zu beurteilen.

In § 280 Abs. 6 dritter Satz BDG 1979 wird von den Öffnungsklauseln in Art. 23 und in Art. 89 Abs. 2 DSGVO Gebrauch gemacht. Es werden die Rechte der betroffenen Personen auf Information, Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch im Rahmen einer Abwägung im jeweiligen Einzelfall beschränkt. Bei der Abwägung ist zu überprüfen, ob diese Rechte voraussichtlich die Verwirklichung der Forschungszwecke oder der statistischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungszwecke oder der statistischen Zwecke notwendig ist. Dadurch soll insbesondere sichergestellt werden, dass die für die wissenschaftlichen oder historischen Forschungszwecke oder die statistischen Zwecke notwendige Vollständigkeit der Daten gewährleistet und nicht durch Ausübung der genannten Rechte der betroffenen Personen ernsthaft beeinträchtigt oder unmöglich gemacht wird. Regelungen zur Auflösung des Personenbezuges durch geeignete technische Mittel tragen insbesondere dem Grundsatz der Datenminimierung und dem Schutz der Rechte und Freiheiten betroffener Personen Rechnung.

In § 280b Abs. 5 bis 8 BDG 1979 wird von der in Art. 23 DSGVO eröffneten Möglichkeit der Beschränkung der Pflichten und Rechte gemäß Art. 5, 12 bis 22 und 34 DSGVO Gebrauch gemacht. Dies erfolgt unter Beachtung des Wesensgehalts der Grundrechte und Grundfreiheiten. Dabei kommen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zur Anwendung. Derartige Beschränkungen von Rechten und Pflichten müssen darüber hinaus der Sicherstellung bestimmter Zwecke dienen, unter denen beispielsweise in Art. 23 Abs. 1 lit. e DSGVO der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“ genannt wird. Daneben können sich solche Beschränkungen beispielsweise auch auf Art. 23 Abs. 1 lit. f und h bis j DSGVO stützen. Die Verarbeitung, Übermittlung und Weiterverarbeitung von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten ist für den öffentlichen Dienst unerlässlich und liegt aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Aufrechterhaltung und dem ordnungsgemäßen und rechtskonformen Funktionieren des öffentlichen Dienstes, insbesondere im Sinne einer Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, selbst im öffentlichen Interesse. Insbesondere ist es erforderlich, dass im öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung besteht und dass die Revisionssicherheit gewährleistet ist. Es ist daher erforderlich und sachgerecht, gewisse Beschränkungen der Rechte der betroffenen Personen vorzunehmen.

Ein Verantwortlicher ist nach der DSGVO zur Berichtigung, Aktualisierung oder Vervollständigung von personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten, die durch ihn verarbeitet werden, verpflichtet. Dies ergibt sich einerseits aus Art. 5 Abs. 1 lit. d DSGVO und andererseits aus dem Recht der betroffenen Person auf Berichtigung gemäß Art. 16 DSGVO. Der Rechtskraft fähige Erledigungen enthalten personenbezogene Daten und unter Umständen auch besondere Kategorien personenbezogener Daten, die grundsätzlich dem Recht auf beziehungsweise der Pflicht zur Berichtigung gemäß den Bestimmungen der DSGVO unterliegen. Da sich daraus ein Spannungsverhältnis zum allgemeinen Konzept der Rechtskraft beziehungsweise der Verjährung ergibt, ist eine Beschränkung des Grundsatzes der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO sowie des Rechtes auf Berichtigung gemäß Art. 16 DSGVO vorgesehen. § 280b Abs. 5 BDG 1979 beschränkt den Grundsatz der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO sowie das Recht auf Berichtigung gemäß Art. 16 DSGVO bei unrichtigen oder unvollständigen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten insoweit, als einer Berichtigung die Rechtskraft oder die Verjährung entgegenstehen, oder wenn ein zumutbarer Rechtsweg besteht oder bestand. Dies dient nicht nur dem Schutz des jeweils vorgesehenen Verfahrens, sondern stellt insbesondere klar, dass das Recht auf Berichtigung auch im Anwendungsbereich der §§ 280 ff BDG 1979 nicht der Umgehung anderer rechtlicher Vorschriften oder eines durch den Gesetzgeber vorgesehenen Rechtsweges dient. Dass eine

nicht inhaltsändernde Stellungnahme abgegeben werden kann, bedeutet, dass im Sinne einer Vervollständigung oder ergänzenden Erklärung zwar von den personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten abweichende Inhalte angeführt werden können, diese Inhalte der personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten gemäß § 280 Abs. 1 BDG 1979 aber aufgrund der Stellungnahme nicht geändert werden dürfen. Die Wahrung der Rechtssicherheit und Rechtsbeständigkeit stellt ein wichtiges Ziel des allgemeinen öffentlichen Interesses dar und daher ist eine Beschränkung im Ausmaß des § 280b Abs. 5 BDG 1979 von Art. 23 Abs. 1 lit. e DSGVO gedeckt.

§ 280b Abs. 6 BDG 1979 stellt klar, dass für zulässig verarbeitete Daten das Recht auf Löschung gemäß Art. 17 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung ausgeschlossen ist. Eine solche Möglichkeit besteht gemäß Art. 17 Abs. 3 DSGVO zur Erfüllung einer rechtlichen Verpflichtung, wie beispielsweise einer Aufbewahrungspflicht, die die Verarbeitung nach dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Zur Aufrechterhaltung des öffentlichen Dienstes und der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten von betroffenen Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten bis zum Ablauf der durch Gesetz oder durch Verordnung bestimmten Frist der Aufbewahrungspflicht erforderlich. Auf Art. 17 Abs. 3 lit. d und e DSGVO wird außerdem hingewiesen. Macht eine betroffene Person glaubhaft, dass die Aufbewahrung ihrer personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten sie erheblich in ihren Rechten beeinträchtigt, so kann auf Antrag der betroffenen Person für die verbleibende Dauer der Aufbewahrungspflicht eine Speicherung ohne Aufbereitung vorgesehen werden, wenn für diesen Zeitraum keine weitere Verarbeitung, Übermittlung oder Weiterverarbeitung vorgesehen ist.

§ 280b Abs. 7 BDG 1979 regelt eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Die Überprüfung der Richtigkeit der personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der betroffenen Person soll nicht dazu führen, dass in den standardisierten IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verarbeitung, Übermittlung und Weiterverarbeitung einzuschränken wäre, was beispielsweise ein momentanes Anhalten der Vorrückung oder eine nicht zeitgerechte Anweisung des zustehenden Bezuges zur Folge haben kann. Alleine das Bestehen dieser möglichen Folgen aufgrund der integrierten Datenverarbeitungssysteme würde neben der Verursachung eines beträchtlichen Verwaltungsaufwandes für viele betroffene Personen die Geltendmachung ihrer Rechte gemäß DSGVO erschweren oder faktisch unmöglich machen, weswegen für den Anwendungsbereich der §§ 280 ff BDG 1979 eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung im erforderlichen Ausmaß sachgerecht ist. Gleiches gilt für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung ist auch im Lichte des wichtigen wirtschaftlichen und finanziellen Interesses des Staates, beispielsweise im Haushalts- und Steuerbereich, erforderlich und sachgerecht im Sinne des Art. 23 Abs. 1 lit. e DSGVO, da etwa die rechtskonforme Abführung von Beiträgen zur Sozialversicherung und der Lohnsteuer, der rechtskonforme Vollzug der Personaladministration, die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung und die Revisionssicherheit wichtige Ziele des allgemeinen öffentlichen Interesses darstellen, deren Schutz die Beschränkung gemäß § 280 Abs. 7 BDG 1979 rechtfertigt.

Aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Verarbeitung der personenbezogenen Daten und besonderen Kategorien personenbezogener Daten der Personen gemäß § 280 Abs. 1 BDG 1979 ist es erforderlich und sachgerecht, das Recht auf Widerspruch gemäß Art. 21 DSGVO in § 280b Abs. 8 BDG 1979 für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung auszuschließen, sofern die betroffene Person nicht Gründe nachweisen kann, die sich aus ihrer besonderen Situation ergeben und die die Ziele der Beschränkung des Rechtes auf Widerspruch überwiegen. Die Erforderlichkeit und Sachlichkeit dieser Beschränkung ergibt sich aus dem überwiegenden, berechtigten öffentlichen Interesse an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des öffentlichen Dienstes, konkret dem rechtskonformen Vollzug der Personaladministration, dem rechtskonformen Abführen von Beiträgen, beispielsweise zur Sozialversicherung und der Lohnsteuer sowie der Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit. Insbesondere ist es erforderlich, dass im öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur

Planstellenbewirtschaftung besteht und dass die Revisionssicherheit gewährleistet ist. Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 1 BDG 1979 erfolgen ausschließlich zu in § 280 Abs. 2 BDG 1979 genannten Zwecken, sofern dies erforderlich ist. Auch für die weiteren Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß den §§ 280 und 280a Abs. 1 und 7 BDG 1979 besteht ein überwiegendes, berechtigtes öffentliches Interesse, wobei auch auf Art. 21 Abs. 6 DSGVO hingewiesen wird. Darüber hinaus würde für den Fall, dass eine betroffene Person ihr Recht auf Widerspruch geltend macht, nicht zuletzt aufgrund der integrierten Datenverarbeitungssysteme mindestens eine weitere Verarbeitung, Übermittlung und Weiterverarbeitung erforderlich werden, was dem grundsätzlichen Anliegen der betroffenen Person zuwiderlaufen würde. Es wird daher eine sachgerechte und erforderliche Beschränkung des Rechtes auf Widerspruch gemäß Art. 21 DSGVO im Sinne des Art. 23 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung vorgeschlagen, sofern nicht eine beschriebene besondere Situation vorliegt. In Fällen, in denen das Widerspruchsrecht nicht gemäß § 280b Abs. 8 BDG 1979 eingeschränkt ist, kann sich direkt aus Art. 21 Abs. 1 letzter Satz und Abs. 6 letzter Satz DSGVO ergeben, dass trotz Widerspruchs eine Verarbeitung, Übermittlung oder Weiterverarbeitung personenbezogener Daten zulässig ist.

Da § 119a Abs. 2 LDG 1984 und § 119h Abs. 2 LLDG 1985 auf § 280b Abs. 4 bis 8 BDG 1979 verweisen, gelten die Ausführungen zu § 280b Abs. 4 bis 8 BDG 1979 sinngemäß auch für diese Bestimmungen.

Die genannten Risiken sind nach Erwägungsgrund 75 DSGVO mit Eintrittswahrscheinlichkeit und Schwere anzugeben. Angesichts der verschwindend geringen Zahl von zwei Verurteilungen nach § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) im Jahr 2016 (Statistik Austria, Gerichtliche Kriminalstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html, [15.03.2018]) sowie einer Zahl von ca. 3,6 Mio. aktiven IT-Systemen in Österreich, ergibt sich eine Wahrscheinlichkeit von unter 1:1 Million, dass sich die von der DSGVO angeführten Risiken oder Nachteile verwirklichen. Die Zahl von 3 610 602 aktiven IT-Systemen ergibt sich aus der Zahl der Privathaushalte, die für das Jahr 2016 mit 3 865 000 beziffert wird (Statistik Austria, Haushaltsstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/bevoelkerung/haushalte_familien_lebensformen/index.html, [15.03.2018]), der Zahl der Unternehmen, die für das Jahr 2015 mit 328 638 beziffert wird (Statistik Austria, Leistungs- und Strukturstatistik 2015, http://www.statistik.at/web_de/statistiken/wirtschaft/unternehmen_arbeitsstaetten/index.html, [15.03.2018]) sowie dem Faktor der IKT-Nutzung der für das Jahr 2016 für private Haushalte mit 85 Prozent und für Unternehmen mit 99 Prozent (Statistik Austria, IKT-Einsatz in Haushalten beziehungsweise Unternehmen, https://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/index.html, [15.03.2018]) beziffert wird.

Im Jahr 2016 (Statistik Austria, Gerichtliche Kriminalstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html, [15.03.2018]) erfolgten 57 Verurteilungen nach § 302 StGB (Missbrauch der Amtsgewalt) und eine Verurteilung nach § 310 StGB (Verletzung des Amtsgeheimnisses). Wie viele der Verurteilungen etwa aufgrund des gezielten Beschaffens personenbezogener Daten oder besonderer Kategorien personenbezogener Daten durch Abfrage in für die Erfüllung dienstlicher Aufgaben eingerichteter Datenbanken oder aufgrund des Ermittelns personenbezogener Daten oder besonderer Kategorien personenbezogener Daten ohne dienstliche Rechtfertigung erfolgten, war nicht feststellbar. Daher kann für die Fälle des Missbrauches der Amtsgewalt sowie der Verletzung des Amtsgeheimnisses keine Wahrscheinlichkeit des Verwirklichens der von der DSGVO angeführten Risiken oder Nachteile angegeben werden.

ABHILFEMAßNAHMEN

Die Datensicherheitsprozesse im IT-Personalmanagement des Bundes orientieren sich an folgenden Normen, Standards, E-Government Konventionen und Empfehlungen:

- ISO 27001, ISO 27002 und ISO 27005 (Informationssicherheit);
- ISO 29100, ISO 29134 und ISO 29151 (Datenschutz);
- ÖNORM S 2109 und DIN 66399-1 (Akten- und Datenvernichtung);
- IT-Grundschutzkataloge (Gefährdungskataloge) des deutschen Bundesamts für Sicherheit in der Informationstechnik;
- Datenschutz-Leitlinien der österreichischen Datenschutzbehörde;
- Datenschutz-Leitlinien der Artikel-29-Datenschutzgruppe.
- BLSG-Konvention „Portalverbund – Grundschutz“

- BLSG-Konvention „Portalverbund – Sicherheitsmaßnahmen“
- BLSG-Konvention „Portalverbund – Verwaltungsprozess für zentrale Dienste“
- BLSG-Konvention „Portalverbundprotokoll Version 2“
- BLSG-Konvention „Sicherheitsklassen – Zugriff von Benutzern auf Anwendungen“
- BLSG-Konvention „Revisionsabfrage im Portalverbund“
- BLSG-Konvention „Datensicherheitsmaßnahmen für Webanwendungen“
- BLSG-Konvention „Common Audit Trail Exchange Format”
- BLSG-Konvention „Sicherheitsstufen – Kommunikation Bürger – Behörde“
- ISK-Vorgabe „Nationale Kryptostrategie“
- ISK-Vorgabe „TLS-Vorgaben für klassifizierte Informationen“
- ISK-Vorgabe „Vorgaben zu E-Mail für klassifizierte Informationen“

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in Erwägungsgrund 78 der DSGVO unter anderem genannt:

– *„Minimierung der Verarbeitung personenbezogener Daten“ und „Verwendungsbeschränkung“*:

Die Minimierung der Verarbeitung personenbezogener Daten ergibt sich unmittelbar aus Art. 5 Abs. 1 lit. c DSGVO. Dort wird die Datenminimierung in dem Sinne geregelt, dass Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Dieser Grundsatz ist in vielfältiger Weise auch im Gesetzestext anzutreffen, insbesondere durch den konsequenten Einsatz des Kriteriums der Erforderlichkeit der jeweiligen Verarbeitung, Übermittlung oder Weiterverarbeitung (vgl. § 79e Abs. 2, 2a und 3, § 79f Abs. 5, § 79g Abs. 1, § 280 Abs. 2, 3 und 5 bis 7 und § 280a Abs. 7 BDG 1979, § 119a Abs. 2 LDG 1984, § 119h Abs. 2 LLDG 1985, § 1a Abs. 1 und 2 und § 105 Abs. 5 PG 1965, § 1a Abs. 1 und 2 BThPG und § 1a Abs. 1 und 2 BB-PG).

Die Beachtung des Grundsatzes der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO, wonach personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, ergibt sich ebenso aus dem Kriterium der Erforderlichkeit sowie aus den bereits beschriebenen Aufbewahrungspflichten und Löschpflichten. So sind etwa Strafregisterauskünfte nach ihrer Überprüfung unverzüglich zu löschen (vgl. § 204 Abs. 8 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG).

§ 280a Abs. 2 bis 5 BDG 1979 enthält Bestimmungen zur Datenaufbewahrung. Bei gemeinsam Verantwortlichen ist dem Grundsatz der Datenminimierung folgend die Aufbewahrungspflicht nur von einem Verantwortlichen wahrzunehmen. Gesetzlich ist eine fünfzehnjährige Frist für personenbezogene Daten und besondere Kategorien personenbezogener Daten vorgesehen. Für Protokolldaten über lesende Zugriffe ist eine dreijährige Frist und für Protokolldaten über inhaltsändernde Zugriffe eine siebenjährige Frist festgelegt. § 280a Abs. 6 BDG 1979 bestimmt, dass eine durch Gesetz oder Verordnung vorgesehene längere Aufbewahrungspflicht oder Archivierung den in § 280 Abs. 2 bis 5 BDG 1979 vorgesehenen Aufbewahrungspflichten vorgeht. Etwaige längere Aufbewahrungspflichten sollen demnach nicht durch die Einführung einer Aufbewahrungspflicht gemäß § 280a BDG 1979 verkürzt werden. Ebenso unberührt bleiben sollen die Löschpflicht von Strafregisterauskünften und die Löschpflicht gemäß § 79e Abs. 2a BDG 1979. Werden jedoch speziellere Fristen für Aufbewahrungspflichten durch den Verantwortlichen oder die gemeinsam Verantwortlichen mittels Verordnung vorgesehen, so gehen diese der jeweiligen Frist der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 BDG 1979 vor. Die Fristen für Protokolldaten über lesende Zugriffe müssen jedoch mindestens ein Jahr und für Protokolldaten über inhaltsändernde Zugriffe mindestens drei Jahre betragen, damit insbesondere die Rechte betroffener Personen nicht durch zu kurze Fristen eingeschränkt werden. Eine durch Gesetz oder Verordnung vorgesehene längere Frist einer Aufbewahrungspflicht oder Archivierung geht gemäß § 280 Abs. 6 BDG 1979 auch einer durch Verordnung gemäß § 280a Abs. 7 BDG 1979 festgesetzten kürzeren Frist vor. Gemeinsam Verantwortliche haben beim Erlassen einer Verordnung gemäß § 280a Abs. 7 BDG 1979 das Einvernehmen herzustellen. Durch die Verordnungsermächtigung in § 280a Abs. 7 BDG 1979 soll insbesondere den Grundsätzen der Speicherbegrenzung und Datenminimierung besonders Rechnung getragen werden.

Der sich aus Art. 5 Abs. 1 lit. b DSGVO ergebende Grundsatz der Zweckbindung ist ebenso durchgehend umgesetzt. Danach dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung zu einem anderen Zweck, der ebenso wie der ursprüngliche Zweck der Verarbeitung durch § 280 Abs. 2 BDG 1979 erfasst sein muss, ist daher nur

möglich, sofern die personenbezogenen Daten oder die besonderen Kategorien personenbezogener Daten zu diesem „neuen“ Zweck ebenfalls erhoben und verarbeitet werden dürften, eine derartige neuerliche Erhebung bereits vorhandener Daten jedoch aus Gründen der Verwaltungsvereinfachung sowie den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit folgend unterbleibt und sofern eine Weiterverarbeitung erfolgen kann und darf. Die in § 280 Abs. 2 BDG 1979 genannten Zwecke dienen dem übergeordneten Zweck der Personaldatenverarbeitung im jeweiligen Rechtsverhältnis und stehen somit in einem engen und manchmal untrennbaren Zusammenhang. Die Datenerhebung erfolgt zwar jeweils zu einem konkreten Zweck, jedoch stets im Hinblick auf die Personaldatenverarbeitung im jeweiligen Rechtsverhältnis. Personenbezogene Daten und besondere Kategorien personenbezogener Daten werden im Rahmen einer Weiterverarbeitung nur insoweit verarbeitet, als eine neuerliche Erhebung der bereits vorhandenen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten möglich wäre. Da Strafregisterauskünfte sowie zu Kontrollzwecken verarbeitete besondere Kategorien personenbezogener Daten nach ihrer Überprüfung unverzüglich zu löschen sind, kann eine Weiterverarbeitung selbiger zu einem anderen Zweck gar nicht in Betracht kommen. Aufgrund der genannten Einschränkungen der Weiterverarbeitung resultieren aus einer Weiterverarbeitung für die betroffene Person keine Folgen, die nicht auch ohne die jeweilige Weiterverarbeitung eingetreten wären. Es gelten aus den genannten Gründen außerdem die gleichen Garantien, die im Falle einer Neuerhebung der personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten gelten würden.

Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken. Die rechtmäßige Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist auf Grundlage des § 280 BDG 1979 zulässig, sofern dies erforderlich ist. Die Erforderlichkeit in diesem Zusammenhang ergibt sich aus der Zusammenschau mit den in Art. 23 Abs. 1 DSGVO genannten Zielen, für die die Verarbeitung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz dieser Ziele darstellen muss. Insbesondere ist hierbei an die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen sowie an den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaates zu denken. Davon abgedeckt sind auch wichtige wirtschaftliche oder finanzielle Interessen des jeweiligen Mitgliedstaates. Insbesondere darf an dieser Stelle auch das wichtige öffentliche Interesse am Funktionieren des öffentlichen Dienstes und an einem rechtskonformen Vollzug der gesetzlichen Vorschriften hervorgehoben werden.

Zu § 280 Abs. 1 und 2 BDG 1979 wird festgehalten, dass eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung und Weiterverarbeitung, sofern nicht ausdrücklich normiert, auf Grundlage des § 280 Abs. 1 und 2 BDG 1979 nicht vorgesehen ist. Von der Ermächtigung des § 280 Abs. 1 und 2 BDG 1979 sind lediglich erforderliche Übermittlungen zwischen den Leiterinnen und Leitern der Zentralstellen erfasst. Darüber hinausgehende Übermittlungen an Leiterinnen oder Leiter der Zentralstellen oder Dritte bleiben von dieser Bestimmung unberührt und sind anhand ihrer jeweiligen Rechtsgrundlage zu beurteilen. Die Dokumentation einer Übermittlung an Dritte, die über eine Übermittlung nach § 280 Abs. 1 erster Satz BDG 1979 hinausgeht, hat zumindest Datum, Uhrzeit, Empfängerin oder Empfänger, die Kategorien und den Umfang der übermittelten personenbezogenen Daten und besonderen Kategorien personenbezogener Daten sowie eine Begründung der Übermittlung unter Hinweis auf die jeweilige Rechtsgrundlage zu enthalten.

Die Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 3 und 5 bis 7 BDG 1979 sowie § 280a Abs. 1, 6 und 7 BDG 1979 sind ebenfalls an die in den Bestimmungen angeführten Zwecke gebunden.

§ 280 Abs. 6 BDG 1979 beinhaltet weiters Regelungen zur unverzüglichen Auflösung des Personenbezuges bei der Verarbeitung von personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten zu statistischen Zwecken oder zu wissenschaftlichen oder historischen Forschungszwecken. Eine Minimierung der Verarbeitung findet daher in der Praxis jedenfalls dann statt, wenn eine Verarbeitung personenbezogener Daten für den beabsichtigten Zweck nicht erforderlich ist, also beispielsweise im Zusammenhang mit statistischen Auswertungen oder der Erstellung von Controllingberichten.

Gemäß § 79e Abs. 3 BDG 1979 dürfen etwa Inhalte übertragener oder zu übertragender Nachrichten nur dann im Sinne des § 79e BDG 1979 kontrolliert werden, wenn dies für die Erreichung der angeführten Zwecke unbedingt erforderlich ist. Weiters wird mit § 79e Abs. 2 BDG 1979 festgelegt, dass zu Kontrollzwecken verarbeitete besondere Kategorien personenbezogener Daten unverzüglich dokumentiert zu löschen sind, sobald eine weitere Verarbeitung zu Kontrollzwecken nicht mehr unbedingt erforderlich ist.

§ 79e Abs. 4 BDG 1979 sieht im Sinne des Regelungskonzeptes der stufenweisen Kontrollverdichtung in Bezug auf die Kontrolle der IKT-Nutzung vor, dass sich vorerst anonyme Kontrollmaßnahmen, bei denen noch kein Rückschluss auf einzelne Bedienstete möglich ist, auf Organisationseinheiten mit mindestens fünf Bediensteten zu beziehen haben. Bei Organisationseinheiten mit weniger als fünf Bediensteten ist für die Durchführung einer Kontrollmaßnahme die jeweils übergeordnete Organisationseinheit miteinzubeziehen. Wenn bestimmte Programme und Anwendungen auch unter Einbeziehung der übergeordneten Organisationseinheiten weniger als fünf Bediensteten zur Verfügung stehen, dürfen Kontrollmaßnahmen auch auf diesen kleineren Bedienstetenkreis bezogen durchgeführt werden.

§ 79f Abs. 5 BDG 1979 regelt beispielsweise ein Weiterverarbeitungsverbot für Daten im dort angeführten Sinn.

Gemäß § 10a Bundes-Personalvertretungsgesetz erfolgt beispielsweise eine Einsichtnahme grundsätzlich nur ins Personalverzeichnis und für darüber hinausgehende Verarbeitungen wird die Zustimmung der oder des betroffenen Bediensteten benötigt.

Bezüglich § 119a LDG 1984 und 119h LLDG 1985 wird auf die Ausführungen zu den §§ 280 ff BDG 1979 verwiesen.

Die Zugriffs- und Berechtigungskonzepte des IT-Personalmanagements entsprechen dem Grundsatz der Beschränkung auf das notwendige Maß.

– *„schnellstmögliche Pseudonymisierung personenbezogener Daten“* (siehe auch Erwägungsgrund 28 DSGVO):

Auf die Ausführungen zu § 79e Abs. 4 BDG 1979 wird verwiesen.

Eine Pseudonymisierung der auf Grundlage des § 280 BDG 1979 erhobenen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten selbst ist nicht möglich, weil im Sinne des jeweiligen Rechtsverhältnisses eine zweifelsfreie Zuordnung sowohl in der analogen, als auch in der digitalen Welt möglich bleiben muss, was auch dem Kriterium der Erforderlichkeit entspricht. Ist eine Auflösung des Personenbezuges durch geeignete technische Mittel (vgl. § 280 Abs. 6 BDG 1979) jedoch möglich, so wird diese insbesondere gemäß den Grundsätzen der Datenminimierung und der Speicherbegrenzung und im Sinne des Art. 32 DSGVO vorgenommen, sofern nicht ohnedies eine Löschung zu erfolgen hat.

Bezüglich § 119a LDG 1984 und 119h LLDG 1985 wird auf die Ausführungen zu den §§ 280 ff BDG 1979 verwiesen.

– *„Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten“ und „Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen“*:

Durch die explizite gesetzliche Regelung der Datenverarbeitung sowie deren Zwecke wird den Anforderungen der Transparenz bereits durch die Kundmachung in hohem Maße Rechnung getragen.

Auf die Informationspflichten gemäß Art. 13 und Art. 14 DSGVO wird an dieser Stelle hingewiesen.

Übt eine betroffene Person ihre Rechte nach der DSGVO gegenüber einem unzuständigen Verantwortlichen aus, so hat dieser sie gemäß § 280b Abs. 4 BDG 1979 an den zuständigen Verantwortlichen zu verweisen. Die Übermittlung von Informationen an die betroffene Person hat unentgeltlich innerhalb eines Monats nach Ausübung eines der genannten Rechte nach der DSGVO direkt schriftlich, gegebenenfalls elektronisch oder in einer anderen, schriftlich dokumentierten Form zu erfolgen. Die Frist kann vor Ablauf nach begründeter Verständigung der betroffenen Person um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Geltendmachungen erforderlich ist. Macht eine betroffene Person ein gemäß § 280b Abs. 5 bis 8 BDG 1979 beschränktes Recht geltend, so ist sie darauf hinzuweisen und die zuständige Datenschutzbeauftragte oder der zuständige Datenschutzbeauftragte ist darüber in Kenntnis zu setzen.

Außerdem wird durch das gemäß Art. 30 DSGVO zu führende Verzeichnis von Verarbeitungstätigkeiten, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, dargestellt, welche Verarbeitungstätigkeiten jeweils vorgenommen werden und der jeweiligen Zuständigkeit unterliegen.

Beispiele für Informationspflichten im Zusammenhang mit betroffenen Personen finden sich etwa in § 79e Abs. 2a, § 79f Abs. 5, § 79g Abs. 6 und 7 sowie § 280 Abs. 3 BDG 1979 oder § 119a Abs. 2 LDG 1984 und 119h Abs. 2 LLDG 1985.

Bezüglich § 119a LDG 1984 und 119h LLDG 1985 wird auf die Ausführungen zu den §§ 280 ff BDG 1979 verwiesen.

Über das ESS-Serviceportal des IT-Personalmanagement erfolgen entsprechende Informationen an die betroffenen Personen, deren personenbezogene Daten oder besondere Kategorien personenbezogener Daten mittels IT-Personalmanagements verarbeitet werden.

– „*Datensicherheitsmaßnahmen*“ (Erwägungsgrund 83 DSGVO):

Durch entsprechende technische und personelle Maßnahmen wird im Einzelfall sichergestellt, dass personenbezogene Daten oder besondere Kategorien personenbezogener Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet und einen entsprechenden Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung bietet, wodurch vor allem dem Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO Rechnung getragen wird. In diesem Zusammenhang wird auch auf Art. 25 DSGVO hingewiesen.

Die Verantwortlichen gemäß § 280 Abs. 1 BDG 1979 und die gemeinsam Verantwortlichen gemäß § 280b Abs. 2 BDG 1979 haben jeweils gemäß Art. 32 bis 34 DSGVO für die Sicherheit der personenbezogenen Daten, der besonderen Kategorien personenbezogener Daten sowie der Protokolldaten zu sorgen. Die Bundeskanzlerin oder der Bundeskanzler ist gemäß § 280a Abs. 7 BDG 1979 ermächtigt, zum Zwecke der rechtskonformen Verfahrensgestaltung, der Fehlerbehebung sowie der Datensicherheit in den von ihr oder ihm bereitgestellten oder betriebenen IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes erforderliche nicht inhaltsändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten durchzuführen. Die Erforderlichkeit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten zu den genannten Zwecken ist eng auszulegen. Datensicherheit bezieht sich nicht nur auf den physischen Zugang zu den Datenverarbeitungssystemen, sondern bedeutet auch, dass sichergestellt wird, dass die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und besonderen Kategorien personenbezogener Daten nur berechtigten Personen ermöglichen und diese Daten nur berechtigten Personen zur Verfügung stehen. Personenbezogene Daten und besondere Kategorien personenbezogener Daten sind vor unrechtmäßigen Verarbeitungen, Übermittlungen oder Weiterverarbeitungen zu schützen, was insbesondere durch entsprechende Protokollierung zu erfolgen hat. Daher ist von dem oder den jeweils Verantwortlichen sicherzustellen, dass bestehende Protokolldaten nicht verändert werden können. Für Bereiche, in denen die Leiterinnen und Leiter der Zentralstellen jeweils mit der Bundeskanzlerin oder dem Bundeskanzler gemeinsam Verantwortliche sind, erfolgt gemäß § 280b Abs. 2 BDG 1979 die Aufteilung der Pflichten unbeschadet der Stellung als gemeinsam Verantwortliche im Sinne der DSGVO durch Verordnung der Bundesregierung. Die Möglichkeit zur Festlegung der jeweiligen Aufgaben der Verantwortlichen durch Rechtsvorschriften der Mitgliedstaaten, denen die Verantwortlichen unterliegen, wird in Art. 26 Abs. 1 DSGVO eröffnet. Dadurch soll vor allem gewährleistet sein, dass betroffene Personen bei der Geltendmachung ihrer Rechte gemäß DSGVO hinsichtlich standardisierter IKT-Lösungen und IT-Verfahren des Personalmanagements des Bundes unabhängig davon, welche Konstellation gemeinsam Verantwortlicher vorliegt, vergleichbar behandelt werden.

Datensicherheitsmaßnahmen werden etwa auch durch Sicherheitsanalysen bei der Programmierung sowie bereits jetzt umgesetzte Rollenkonzepte und die damit eindeutige Identifikation der oder des jeweiligen Verarbeitenden getroffen.

Es wird außerdem an dieser Stelle auf die Regelungen zu Auftragsverarbeitern in Art. 28 DSGVO hingewiesen.

Gemäß Art. 35 Abs. 10 DSGVO ist eine Datenschutz-Folgenabschätzung im Zuge von Gesetzgebungsverfahren zulässig. Die konkret eingesetzte Infrastruktur wird jedoch typischerweise nicht gesetzlich geregelt, weswegen an dieser Stelle auf die Einhaltung der Maßnahmen gemäß Art. 25 und Art. 32 DSGVO hingewiesen wird. Durch die Publikation der angeführten Bestimmungen in den jeweiligen gesetzlichen Grundlagen als Bundesgesetz im Bundesgesetzblatt sowie der parlamentarischen Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe für die zulässige Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten sowie die zum Begutachtungsentwurf erfolgten Stellungnahmen von der Öffentlichkeit kostenlos eingesehen und nachvollzogen werden. Im Rahmen des erfolgten Begutachtungsverfahrens wurde insbesondere der Datenschutzbehörde, den Datenschutzbeauftragten, den betroffenen Personen und den Verantwortlichen die Möglichkeit zur Stellungnahme eingeräumt. Durch die Abgabe von Stellungnahmen erfolgte eine aktive Mitwirkung an der Gestaltung des Gesetzestextes,

um die Vereinbarkeit der geplanten Verarbeitungen, Übermittlungen und Weiterverarbeitungen mit der DSGVO sicherzustellen.

Weiters trägt die Benennung einer oder eines jeweils zuständigen Datenschutzbeauftragten maßgeblich zur Datensicherheit bei. Hinzu kommen beispielsweise entsprechende Schulungen, Handbücher, Sicherheitskonzepte oder gegebenenfalls Weisungen, die auf den jeweiligen Einzelfall abstellen.

Bezüglich § 119a LDG 1984 und 119h LLDG 1985 wird auf die Ausführungen zu den §§ 280 ff BDG 1979 verwiesen.

Außerdem bestehen Verarbeitungs-, Übermittlungs- und Weiterverarbeitungsmöglichkeiten stets nur für Personen, die sich in ihrem jeweiligen Rechtsverhältnis entsprechend bewährt und als verlässlich erwiesen haben. Insbesondere die Bestimmungen zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit und zu Kontrollmaßnahmen im Sinne des 5a. Unterabschnitts des BDG 1979 bewirken durch die dort gesetzten Maßnahmen ebenso eine Erhöhung der Datensicherheit.