1 von 29

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Das geltende Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, setzt 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 innerstaatliches Recht um.

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, beschlossen. Die Datenschutz-Grundverordnung (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 auf.

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 neuen Datenschutzgesetz (DSG) erfolgt, werden Öffnungsklauseln nur zu einem geringen Teil direkt im neuen DSG geregelt bzw. handelt es sich um Regelungsspielräume, die im neuen DSG bewusst nicht geregelt werden, da die DSGVO bereits eine Grundregel enthält, die – als allgemeiner Ansatz – grundsätzlich auch im nationalen Recht übernommen werden soll (zB Art. 8 Abs. 1 DSGVO hinsichtlich der Altersgrenze für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft). Der überwiegende Teil der Öffnungsklauseln fällt jedoch nicht in den Bereich der allgemeinen Angelegenheiten des Datenschutzes, deshalb werden diese nicht im neuen DSG geregelt. Jedoch kann – soweit erforderlich – in spezifischen Materiengesetzen eine entsprechende Festlegung erfolgen (zB Art. 23 und 88 DSGVO).

Aus diesen Gründen sind umfassende Änderungen im innerstaatlichen Datenschutzrecht erforderlich, die durch die Erlassung eines neuen DSG vorgenommen werden sollen. Dabei sollen – entsprechend der allgemeinen unionsrechtlichen Vorgaben für Rechtsakte in Verordnungsform – nur die unbedingt erforderlichen Regelungen der Verordnung im innerstaatlichen Recht durchgeführt werden, da die Verordnung in allen sonstigen Teilen ohnedies unmittelbar gilt und ein darüber hinausgehendes Abschreiben von Teilen der Verordnung im Hinblick auf das unionsrechtliche Transformationsverbot nicht zulässig wäre. Hinsichtlich der ausnahmsweise zulässigen Transformation wird auf den Erwägungsgrund 8 der DSGVO verwiesen: Wenn in der DSGVO Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.

Weiters ist im DSG 2000 auch der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. Nr. L 350 vom 27.11.2008 S. 60, umgesetzt. Dieser Rahmenbeschluss wird durch 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, aufgehoben.

Die Richtlinie (EU) 2016/680 bedarf einer Umsetzung ins innerstaatliche Recht. Nachdem der Rahmenbeschluss bisher im DSG 2000 umgesetzt ist, soll die Richtlinie auch im neuen DSG in einem eigenen Hauptstück geregelt werden. Dabei soll im Rahmen der Umsetzung – soweit möglich – auf die zum Teil wortgleichen Regelungen in der DSGVO sowie auf die Durchführungsregelungen zur DSGVO (zB hinsichtlich der Einrichtung der Datenschutzbehörde) verwiesen werden und damit eine möglichst schlanke Umsetzung der Richtlinie erreicht werden. Weiters soll das für diesen Bereich bisher im DSG 2000 festgelegte und innerstaatlich langjährig etablierte Datenschutzniveau im Rahmen der vorzunehmenden Richtlinienumsetzung nicht abgesenkt werden. Wie auch schon nach der geltenden Rechtslage sollen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (leges speciales) den allgemeinen Regelungen des neuen DSG vorgehen.

Neben der Durchführung bzw. Umsetzung der beiden Unionsrechtsakte soll auch weiterhin ein Grundrecht auf Datenschutz in angepasster Form im DSG verankert werden.

Die Mitgliedstaaten können gemäß Art. 6 Abs. 2 DSGVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung 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 rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX der DSGVO. In diesem Rahmen sollen die im DSG 2000 geregelten besonderen Verwendungszwecke von Daten (zB §§ 47 bis 48a DSG 2000) und Regelungen zur Videoüberwachung (vgl. §§ 50a bis 50e DSG 2000) ins neue DSG aufgenommen und im Zuge dessen an die geänderten Erfordernisse angepasst werden. Im Rahmen dieser Vorgaben der DSGVO können auch spezifische Datenverarbeitungen in Materiengesetzen geregelt werden; bestehende Regelungen müssen – soweit sie den Vorgaben der DSGVO nicht entsprechen – angepasst werden. Eine allgemeine Festlegung der Kriterien für die Zulässigkeit von Datenverarbeitungen – wie sie bisher in §§ 8 und 9 DSG 2000 geregelt ist –, erscheint im Lichte der unmittelbaren Geltung der DSGVO und vor dem Hintergrund des Transformationsverbots jedoch nicht mehr zulässig.

Darüber hinaus enthält die DSGVO in Kapitel IX „Vorschriften für besondere Verarbeitungssituationen“. Für diese Verarbeitungssituationen können die Mitgliedstaaten grundsätzlich spezifischere Vorschriften erlassen. Neben der Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit (Art. 85 DSGVO) umfasst dies etwa auch die Datenverarbeitung im Beschäftigungskontext (Art. 88 DSGVO). Die letztgenannte Bestimmung sieht die Möglichkeit vor, durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten vorzusehen.

Weitere Änderungen betreffen die Kompetenzrechtslage auf dem Gebiet des Datenschutzes. Die derzeitige Einschränkung der Gesetzgebungszuständigkeit des Bundes auf den Schutz personenbezogener Daten im automationsunterstützten Datenverkehr soll nun im neuen DSG entfallen. Dadurch soll der Bund in die Lage versetzt werden, die DSGVO und die Richtlinie (EU) 2016/680 einheitlich und vollständig, also auch hinsichtlich manueller personenbezogener Dateien durchzuführen bzw. umzusetzen.

Mit Inkrafttreten des neuen DSG soll das DSG 2000 samt den darauf beruhenden Verordnungen aufgehoben werden.

Kompetenzgrundlage:

Der vorliegende Entwurf stützt sich auf Art. 10 Abs. 1 Z 1 B-VG.

Besonderheiten des Normerzeugungsverfahrens:

Der Entwurf kann gemäß Art. 44 Abs. 1 B-VG vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden und bedarf überdies gemäß Art. 44 Abs. 2 B-VG der in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen zu erteilenden Zustimmung des Bundesrates.

Besonderer Teil

Zu Artikel 1 (Änderung des Bundes-Verfassungsgesetzes)

Zu den Z 1 bis 3:

Im Sinne der Konzentration aller Kompetenzbestimmungen im B-VG sollen die derzeit in § 2 DSG 2000 enthaltenen kompetenzrechtlichen Regelungen in das B-VG in modifizierter Form integriert werden.

Die bisherige Kompetenzrechtslage auf dem Gebiet des Datenschutzes erwies sich vor allem seit Inkrafttreten der Richtlinie 95/46/EG, die sowohl für automationsunterstützt als auch für konventionell (manuell) in einer Datei geführte Datenanwendungen gilt, als unzweckmäßig. Infolge der zwischen Bund und Ländern geteilten Gesetzgebungskompetenz musste diese Richtlinie durch das DSG 2000 und eigene Datenschutzgesetze der Länder umgesetzt werden, wobei der den Ländern – in Folge der Vorgaben der Richtlinie und des Grundrechts auf Datenschutz gemäß § 1 DSG 2000 – verbliebene Gestaltungsspielraum äußerst gering war.

Die bisher in § 2 Abs. 1 DSG 2000 enthaltene Einschränkung der Gesetzgebungszuständigkeit des Bundes auf den Schutz personenbezogener Daten im automationsunterstützten Datenverkehr soll nun im

neuen DSG entfallen. Dadurch soll der Bund in die Lage versetzt werden, die DSGVO und die Richtlinie (EU) 2016/680 einheitlich und vollständig, also auch hinsichtlich manueller personenbezogener Dateien durchzuführen bzw. umzusetzen.

Durch die Einschränkung auf allgemeine Angelegenheiten des Schutzes personenbezogener Daten soll die Zuständigkeit zur Erlassung von auf einen bestimmten Gegenstand bezogenen datenschutzrechtlichen Regelungen – wie bisher auch – unberührt bleiben. Die allgemeinen Angelegenheiten des Schutzes personenbezogener Daten werden auf den neuen Kompetenztatbestand in Art. 10 Abs. 1 Z 13 gestützt im neuen DSG geregelt; hingegen sollen die spezifischen datenschutzrechtlichen Regelungen weiterhin auf die Kompetenztatbestände der jeweiligen Materie gestützt werden (materienspezifischer Datenschutz als Annexmaterie).

Weiters können auch spezifische bundesgesetzliche Datenverarbeitungen als datenschutzrechtliche Annexmaterie erlassen werden (zB datenschutzrechtliche Regelungen im Gesundheitstelematikgesetz 2012 (GTelG 2012), BGBl. I Nr. 111/2012, und im Transparenzdatenbankgesetz 2012 (TDBG 2012), BGBl. I Nr. 99/2012).

Die landesgesetzlichen Vorschriften in den allgemeinen Angelegenheiten des Datenschutzes in Bezug auf den nicht-automationsunterstützten Datenverkehr treten außer Kraft; davon umfasst sind folgende Landesgesetze bzw. Teile von Landesgesetzen: Burgenländisches Datenschutzgesetz (Bgld. DSG), LGBl. Nr. 87/2005; Kärntner Informations- und Statistikgesetz (K-ISG), LGBl. Nr. 70/2005; NÖ Datenschutzgesetz, LGBl. 0901-2; Oö. Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz, LGBl. Nr. 46/1988; Salzburger Gesetz über Auskunftspflicht, Dokumentenweiterverwendung, Datenschutz, Landesstatistik und Geodateninfrastruktur (ADDSG-Gesetz), LGBl. Nr. 73/1988; Steiermärkisches Datenschutzgesetz (StDSG), LGBl. Nr. 39/2001; Tiroler Datenschutzgesetz 2014 (TDSG 2014), LGBl. Nr. 158/2013; Vorarlberger Landes-Datenschutzgesetz, LGBl. Nr. 19/2000; Wiener Datenschutzgesetz (Wr. DSG), LGBl. Nr. 125/2001.

Zudem soll auch die Vollziehung des Datenschutzrechts zur Gänze beim Bund liegen und von diesem in unmittelbarer Bundesverwaltung (Art. 102 Abs. 2 B-VG) vollzogen werden können.

Keine Vollziehung des Datenschutzrechts stellt die bloße Verarbeitung von personenbezogenen Daten durch Länder und Gemeinden als Verantwortliche dar (so zutreffend auch *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung [2014], 339 ff, 341). Da es für die faktische Handhabung personenbezogener Daten durch Behörden insofern keiner allgemeinen datenschutzrechtlichen Vollzugskompetenz, sondern lediglich einer Zuständigkeit aus einem „Materiengesetz“ bedarf, und der Vollzug des DSG bzw. der DSGVO ausschließlich bei der unabhängigen Aufsichtsbehörden liegen soll, hat § 2 Abs. 2 DSG 2000 keine Entsprechung im künftigen DSG.

Zu Artikel 2 (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG))

Zu § 1:

In § 1 soll das Grundrecht auf Datenschutz im Verfassungsrang verankert werden. Das bereits in § 1 DSG 2000 verankerte Grundrecht und Art. 8 Abs. 2 EMRK dienen hierbei als Basis. Jedoch soll die komplexe Formulierung des § 1 Abs. 2 DSG 2000, die in der Praxis zahlreiche Fragestellungen aufgeworfen hat, vermieden werden und eine verständlichere Ausgestaltung der Voraussetzungen für einen Eingriff in das Grundrecht vorgesehen werden. Weiters wird von der DSGVO die juristische Person nicht erfasst; demgemäß soll das Grundrecht auch nur natürliche Personen umfassen. Weiterhin beibehalten werden soll die Drittwirkung des Grundrechts, die sich schon aus der bisherigen Formulierung des § 1 Abs. 1 DSG 2000 ergeben hat und nun auch in Abs. 3 ausdrücklich geregelt wird.

Im Grundrecht soll auf das Recht auf Löschung unzulässigerweise verarbeiteter Daten abgestellt werden. Zwar kennt die DSGVO auch ein Recht auf Beschränkung (statt Löschung); dies erscheint jedoch nicht in jedem Fall als gleichwertige Alternative zum Löschungsrecht.

Eine gesetzliche Grundlage nach § 1 Abs. 2 ist ein Gesetz oder ein Staatsvertrag, der unmittelbar anwendbar ist. Die gesetzliche Grundlage muss ausreichend präzise – also für jedermann vorhersehbar – sein. Ein Gesetz, das die Verarbeitung personenbezogener Daten regelt, hat gemäß den Vorgaben des Art. 8 Abs. 2 der Richtlinie (EU) 2016/680 zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung zu enthalten. Datenverarbeitungen im Rahmen der Vollziehung hoheitlicher oder schlicht hoheitlicher Aufgaben benötigen eine gesonderte gesetzliche Rechtsgrundlage (§ 1 DSG und Art. 18 B-VG).

Darüber hinaus müssen Bestimmungen über die Speicherung personenbezogener Daten gemäß den Vorgaben des Art. 5 der Richtlinie (EU) 2016/680 im Hinblick auf den angestrebten Zweck verhältnismäßige Fristen für die Speicherung bzw. die regelmäßige Überprüfung der Notwendigkeit der Speicherung vorsehen. Diese Regelungen – ebenso wie die verfahrensrechtlichen Vorkehrungen zur Einhaltung dieser Fristen – müssen in den entsprechenden Materiengesetzen, die die Datenverarbeitung regeln, getroffen werden.

Eingriffe in das Grundrecht sind mit Einwilligung der betroffenen Person oder in dessen lebenswichtigem Interesse zulässig. Die „Einwilligung“ in § 1 Abs. 2 soll der „Einwilligung“ nach Art. 4 Z 11 DSGVO entsprechen. Eine Einwilligung der betroffenen Person ist demnach jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Darüber hinaus können Eingriffe im öffentlichen Interesse aufgrund einer gesetzlichen Grundlage oder im überwiegenden berechtigten Interesse eines anderen erfolgen. Ausschließlich diese vier Eingriffstatbestände in das Grundrecht auf Datenschutz sollen zulässig sein und sind gleichrangig. Für Eingriffe im öffentlichen Interesse ist eine gesetzliche Grundlage erforderlich. Auch Gesetze, die eine Interessenabwägung zugunsten oder zulasten Privater vornehmen (zB Verarbeitung von genetischen Daten durch Versicherungen) können im öffentlichen Interesse liegen.

Eingriffe aufgrund eines überwiegenden berechtigten Interesses eines anderen benötigen hingegen nicht zwingend eine gesetzliche Grundlage. Besondere gesetzliche Regelungen zur Einwilligung (zB § 17 Abs. 2 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) ebenso wie das absolute Verbot einer Einwilligung (zB § 67 des Gentechnikgesetzes (GTG), BGBl. Nr. 510/1994) bleiben weiterhin zulässig.

Auch im Falle zulässiger Verarbeitung von vom Abs. 1 umfassten Daten darf der Eingriff in das Grundrecht jeweils nur dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Im Übrigen gilt Art. 8 Abs. 2 der Charta der Grundrechte der Europäischen Union, ABl. C 83 vom 30.3.2010, S. 389, auch ohne ausdrückliche Anordnung für diesen Bereich.

Zu § 2:

§ 2 legt den sachlichen Anwendungsbereich fest. Der räumliche Anwendungsbereich wird unmittelbar in der DSGVO festgelegt.

Die DSGVO gilt gemäß Art. 2 Abs. 1 DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Um auch Datenverarbeitungen außerhalb des Anwendungsbereichs des Unionsrechts zu erfassen (Art. 2 Abs. 2 lit. a DSGVO), wird die DSGVO auch auf diesen Bereich für anwendbar erklärt. Dies soll nur dort nicht gelten, wo im 3. Hauptstück dieses Bundesgesetzes spezifischere Bestimmungen vorgesehen sind.

Zu § 3:

Im DSG 2000 ist derzeit vorgesehen, dass dann, wenn die Löschung oder Richtigstellung von personenbezogenen Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, die zu löschenden personenbezogenen Daten für den Zugriff zu sperren und die zu berichtigenden personenbezogenen Daten mit einer berichtigenden Anmerkung zu versehen sind (§ 27 Abs. 6 DSG 2000). Die DSGVO trifft für einen solchen Fall keine ausdrückliche Vorsorge. Insbesondere bei einer etwa aus Sicherheitsgründen weit verteilten Speicherung von personenbezogenen Daten kann es sich im Einzelfall als schwierig erweisen, einzelne Datensätze sofort aus sämtlichen Kopien zu entfernen. In diesem Lichte erscheint die Beibehaltung einer technikneutral formulierten, adaptierten Fassung des bisherigen § 27 Abs. 6 DSG 2000 sachgerecht.

Zu § 4:

Die Voraussetzungen für die Benennung eines Datenschutzbeauftragten werden in Art. 37 DSGVO unmittelbar anwendbar festgelegt und dürfen daher nicht in das DSG übernommen werden. Nach Art. 37 Abs. 1 DSGVO benennen der Verantwortliche und der Auftragsverarbeiter auf jeden Fall einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln), die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige

und systematische Überwachung von betroffenen Personen erforderlich machen, oder die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht.

Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann. Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben. Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Der Datenschutzbeauftragte und die für ihn tätigen Personen (zB Mitarbeiter des Datenschutzbeauftragten) sind – soweit sie nicht besonderen Geheimhaltungsregelungen unterliegen (zB für Ärzte, Rechtsanwälte oder Notare oder für öffentliche Bedienstete allgemein die Amtsverschwiegenheit) – bei der Erfüllung der Aufgaben in jedem Fall an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Insbesondere sind sie damit auch zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie nicht davon durch die betroffene Person befreit werden. Um das originäre Aussageverweigerungsrecht nicht zu unterlaufen, liegt die Entscheidung über die Inanspruchnahme oder Nichtinanspruchnahme dieses Rechts jeweils bei der Person, der das gesetzliche Aussageverweigerungsrecht zusteht. Zugunsten Letzterer bestehende Beschlagnahmeverbote (vgl. § 157 Abs. 2 StPO) müssen auf den Datenschutzbeauftragten erstreckt werden, um eine Umgehung zu verhindern.

Die Verschwiegenheitspflicht des Datenschutzbeauftragten gilt nicht gegenüber der Datenschutzbehörde.

Zu § 5:

§ 5 enthält zusätzliche Sonderbestimmungen für den Datenschutzbeauftragten im öffentlichen Bereich. Nicht vom Anwendungsbereich des § 5 erfasst sein sollen Verantwortliche gemäß § 15 Abs. 1 Z 2.

Um ein einheitliches und koordiniertes Vorgehen in Datenschutzangelegenheiten zu gewährleisten, sollen die Datenschutzbeauftragten der Bundesministerien regelmäßig zu Sitzungen zusammenzufinden. Es wird davon ausgegangen, dass auch ein Vertreter des Datenschutzrates einzubinden ist. Dem Bundeskanzleramt obliegt nach dem 2. Teil, Abschnitt A, der Anlage zum Bundesministeriengesetz 1986 (BMG), BGBl. Nr. 76/1986, ua. die Koordination der gesamten Verwaltung des Bundes, soweit sie nicht in den Wirkungsbereich eines anderen Bundesministeriums fällt. Demgemäß sind die Sitzungen der Datenschutzbeauftragten der Bundesministerien vom Bundeskanzleramt zu koordinieren.

Gemäß Art. 38 Abs. 6 DSGVO kann der Datenschutzbeauftragte zwar auch andere Aufgaben und Pflichten wahrnehmen, der Verantwortliche oder der Auftragsverarbeiter muss jedoch sicherstellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Daraus folgt auch, dass dem Datenschutzbeauftragten im Falle der zusätzlichen Betrauung mit anderen Aufgaben ausreichend Zeit für Erfüllung seiner Aufgaben als Datenschutzbeauftragter gegeben wird.

Die Weisungsfreistellung des Datenschutzbeauftragten im öffentlichen Bereich stützt sich auf Art. 20 Abs. 2 Z 8 B-VG. Hinsichtlich der Grenzen des gemäß Art. 20 Abs. 2 B-VG vorzusehenden Unterrichtungsrechts wird auf Art. 38 Abs. 3 DSGVO verwiesen.

Im Wirkungsbereich von Bundesministerien bestellte Datenschutzbeauftragte müssen dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören. Eine Bestellung von externen Datenschutzbeauftragten ist unzulässig.

Zu § 6:

Mangels einer expliziten Regelung des Datengeheimnisses in der DSGVO sollen die Regelungen des § 15 DSG 2000 inhaltlich ins neue DSG übernommen werden. Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Verantwortliche und Auftragsverarbeiter dürfen Anordnungen zur Übermittlung von personenbezogenen Daten nur erteilen, wenn dies zulässig ist.

Die Regelung des § 6 soll – wie auch bereits die vergleichbare Regelung in § 15 DSG 2000 – sowohl für Verantwortliche (und Auftragsverarbeiter) des privaten Bereichs als auch für Verantwortliche (und Auftragsverarbeiter) des öffentlichen Bereichs sowie für deren Mitarbeiter gelten.

Zu § 7:

Die DSGVO erfordert aufgrund ihrer unmittelbaren Gültigkeit keine Umsetzung in das nationale Recht des Mitgliedstaats. Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht des Mitgliedstaats vorgesehen sind, können die Mitgliedstaaten jedoch – wie in Erwägungsgrund 8 der DSGVO ausgeführt – Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen. Im Rahmen dieser Vorgaben soll die Durchführung von Kapitel VI der DSGVO zu den unabhängigen Aufsichtsbehörden im DSG nur dort Regelungen vorsehen, wo sie tatsächlich erforderlich sind. Nicht durchführungsbedürftig sind im Kapitel VI etwa Art. 55 und 56 DSGVO. Anzumerken ist im weiteren Zusammenhang auch, dass Art. 54 Abs. 2 DSGVO bereits unmittelbar anwendbar die Verschwiegenheitspflicht festlegt. Darüber hinaus gilt für die betroffenen Personen auch die Amtsverschwiegenheit. Insofern ist eine Durchführung in Form einer Wiederholung des Art. 54 Abs. 2 DSGVO nicht erforderlich.

Jeder Mitgliedstaat sieht gemäß Art. 51 Abs. 1 DSGVO vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind. Diese Vorgaben müssen nicht durchgeführt werden, sondern gelten unmittelbar.

Art. 54 Abs. 1 DSGVO legt den Mitgliedstaaten jedoch auf, die in den lit. a bis f genannten Vorgaben durch Rechtsvorschriften im nationalen Recht vorzusehen. § 7 Abs. 1 legt in diesem Sinne die Datenschutzbehörde als einzige nationale Aufsichtsbehörde gemäß Art. 51 DSGVO fest. Diesbezüglich ist von einer Kontinuität der nach den Vorgaben des DSG 2000 eingerichteten Datenschutzbehörde auszugehen. Mit Geltung der DSGVO (25. Mai 2018) soll die bestehende Datenschutzbehörde somit nationale Aufsichtsbehörde gemäß Art. 51 DSGVO werden.

Auch organisatorisch soll die Struktur der mit der DSG-Novelle 2014, BGBl. I Nr. 83/2013, eingerichteten Datenschutzbehörde beibehalten werden. Die Datenschutzbehörde soll somit als monokratische Behörde fortgeführt werden, der ein Leiter vorsteht. Der Stellvertreter des Leiters der Datenschutzbehörde vertritt den Leiter der Datenschutzbehörde in dessen Abwesenheit.

Der Fortsetzung der laufenden Funktionsperiode der Leitung der Datenschutzbehörde wird in § 76 geregelt.

Für die Ausübung der in der DSGVO festgelegten Aufgaben und Befugnisse gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung ist eine Verfassungsbestimmung erforderlich. Die in § 35 Abs. 2 DSG 2000 geregelte Verfassungsbestimmung soll dementsprechend in das neue DSG übernommen werden.

Zu § 8:

Art. 52 DSGVO regelt die Vorgaben für die Unabhängigkeit der Aufsichtsbehörde. Demnach handelt jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.

Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß der DSGVO weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen. Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Diese in Art. 52 Abs. 1 bis 3 DSGVO geregelten Vorgaben erfordern keine zusätzlichen Durchführungsmaßnahmen im nationalen Recht.

Durchführungsbedürftig sind hingegen Art. 52 Abs. 4 bis 6 DSGVO, die sich direkt an die Mitgliedstaaten richten. § 8 soll diesbezüglich die Vorgaben des Art. 52 Abs. 5 DSGVO durchführen und entspricht inhaltlich § 37 Abs. 2 DSG 2000, der regelt, dass die Datenschutzbehörde Dienstbehörde und Personalstelle ist.

Die Vorgaben des Art. 52 Abs. 4 DSGVO, dass hinsichtlich der Ausstattung der Datenschutzbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können, richtet sich nach weiteren materienspezifischen Regelungen. Die Verpflichtung sicherzustellen, dass die Datenschutzbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen

ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können, ergibt sich unmittelbar aus der DSGVO und wäre in den jeweiligen Gesetzen (zB Bundesfinanzgesetz) entsprechend vorzusehen.

Im Übrigen kann der Leiter der Datenschutzbehörde sein eigenes Personal auswählen, das ausschließlich seiner Leitung untersteht.

Art. 52 Abs. 6 DSGVO, der eine Finanzkontrolle der Aufsichtsbehörde verlangt, soll ebenfalls nicht unmittelbar im DSG geregelt werden, da sich derartige Regelungen bereits aus dem Rechnungshofgesetz 1948 (RHG), BGBl. Nr. 144/1948, ergeben. Der Rechnungshof hat bei der Prüfung der Datenschutzbehörde die in Art. 52 Abs. 6 DSGVO festgelegten Grundsätze einzuhalten.

Im nationalen Recht müssen hingegen aufgrund des Art. 54 Abs. 1 lit. f DSGVO insbesondere auch die Verbote von Handlungen und beruflichen Tätigkeiten geregelt werden. Dies wird in § 8 Abs. 2 – unbeschadet der unmittelbaren Geltung des Art. 52 Abs. 3 DSGVO – im Detail durchgeführt. Zur Durchführung des Art. 54 Abs. 1 lit. f DSGVO ist überdies anzumerken, dass sich die Pflichten und Unvereinbarkeiten der Bediensteten zum Teil auch bereits aus dem Dienstrecht ergeben.

§ 8 Abs. 3 entspricht inhaltlich weitgehend dem bisherigen § 37 Abs. 3 DSG 2000; im Sinne einer unionsrechtskonformen Auslegung des Art. 20 Abs. 2 B-VG (siehe das Urteil des EuGH vom 16. Oktober 2012 in der Rs C-614/10 zur Datenschutz-Richtlinie) wird das Unterrichtungsrecht dahingehend eingeschränkt, dass die Ausübung dieses Rechts den Vorgaben für die Unabhängigkeit in Art. 52 DSGVO nicht widersprechen darf.

Aufgrund des § 7 Abs. 2 letzter Satz gelten für den Stellvertreter des Leiters insbesondere auch die Vorgaben des § 8.

Zu § 9:

Nach Art. 53 Abs. 1 DSGVO müssen die Mitgliedstaaten vorsehen, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar vom Parlament, von der Regierung, vom Staatsoberhaupt oder von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird. Weiters sehen Art. 54 Abs. 1 lit. c, d und e DSGVO vor, dass die Mitgliedstaaten die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde durch Rechtsvorschriften regeln, eine Amtszeit von mindestens vier Jahren festlegen und regeln, ob das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können. Diese Vorgaben sollen in Abs. 1 durchgeführt werden. Dabei werden inhaltlich die in § 36 Abs. 1 DSG 2000 geregelten Vorgaben weitgehend übernommen. Auf die Ausschreibung finden die Regelungen des Ausschreibungsgesetzes 1989 (AusG), BGBl. Nr. 85/1989, Anwendung. Eine – auch mehrmalige – Wiederbestellung zum Leiter der Datenschutzbehörde soll zulässig sein.

Bereits aufgrund des Art. 53 Abs. 2 DSGVO hat jedes Mitglied über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten zu verfügen. Art. 54 Abs. 1 lit. b legt den Mitgliedstaaten jedoch auf, durch Rechtsvorschriften die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde vorzusehen. Diese Vorgaben werden durch Abs. 2 durchgeführt, der inhaltlich § 36 Abs. 2 DSG 2000 entspricht.

Mit Abs. 3 wird hinsichtlich von verbotenen Handlungen und beruflichen Tätigkeiten Art. 54 Abs. 1 lit. f durchgeführt. Für die Berechnung der Zwei-Jahres-Frist gemäß Abs. 3 Z 2 ist – wie bereits bei der inhaltsgleichen Regelung in § 36 Abs. 3 Z 2 DSG 2000 – auf den Zeitpunkt der Bestellung abzustellen.

Zwar regelt Art. 53 Abs. 4 DSGVO die Enthebung eines Mitgliedes von seinem Amt; allerdings bedarf es einer nationalen Regelung, welches Organ diese Enthebung vornehmen soll. Dementsprechend soll die Enthebung des Leiters sowie auch des Stellvertreters nach Abs. 4 auf Vorschlag der Bundesregierung durch den Bundespräsidenten vorgenommen werden.

Der Bundespräsident soll nach Abs. 5 auf Vorschlag der Bundesregierung einen Stellvertreter für den Leiter der Datenschutzbehörde bestellen. Für diesen sollen dieselben Regelungen für die Bestellung, die Unvereinbarkeit, die Beendigung der Funktion und Neubestellung wie für den Leiter der Datenschutzbehörde gelten.

Im Übrigen finden aufgrund der allgemeinen Anordnung in § 7 Abs. 2 auf den Stellvertreter des Leiters der Datenschutzbehörde die Regelungen des Leiters der Datenschutzbehörde sinngemäß Anwendung.

Zu § 10:

Die Aufgaben der Datenschutzbehörde ergeben sich unmittelbar aus der DSGVO (so etwa aufgrund ausdrücklicher Anordnung der Aufgaben in Art. 57 DSGVO). Die dort festgelegten Aufgaben bedürften

weitgehend keiner Durchführung ins nationale Recht. Dies betrifft etwa die Verpflichtung der Datenschutzbehörde, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären (Art. 57 Abs. 1 lit. b DSGVO). Weiters obliegt der Datenschutzbehörde eine der Behördentätigkeit vorgelagerte und begleitende Beratungstätigkeit. Eine Befugnis zur Information der Öffentlichkeit ergibt sich zudem unmittelbar aus Art. 58 Abs. 3 lit. b DSGVO.

Hingegen besteht bei der in Art. 57 Abs. 1 lit. c DSGVO nur allgemein festgelegten Beratungstätigkeit ein gewisser Konkretisierungsbedarf, der in Abs. 1 vorgenommen wird.

Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören. Dies setzt auch Art. 36 Abs. 4 und Art. 57 Abs. 1 lit. c DSGVO um und wird in der Praxis vielfach im Zuge des Begutachtungsverfahrens erfolgen. Darunter können etwa auch Verordnungen von Anstalten des öffentlichen Rechts mit eigener Rechtspersönlichkeit auf Bundesebene, beispielsweise Verordnungen der e-Control sowie der Finanzmarktaufsicht, fallen. Zu Fragen des Datenschutzes gehören auch allgemeine Aspekte der IT- und Cybersicherheit.

Zudem kann sich die Datenschutzbehörde – wie in Art. 57 Abs. 3 lit. b DSGVO vorgesehen – zum Zwecke der Förderung der Bewusstseinsbildung in Datenschutzfragen an die Öffentlichkeit wenden.

Gemäß Art. 57 Abs. 1 lit. k DSGVO hat die Datenschutzbehörde eine Liste der Verarbeitungsarten zu erstellen und zu führen, für die gemäß Art. 35 Abs. 4 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen ist. Durch Abs. 2 soll aus Gründen der Transparenz, Nachvollziehbarkeit und Rechtssicherheit vorgegeben werden, dass diese Liste von der Datenschutzbehörde im Wege einer Verordnung kundzumachen ist; dies soll auch für die Liste nach Art. 35 Abs. 5 DSGVO angeordnet werden.

Aus den oben dargelegten Gründen sieht Abs. 3 hinsichtlich der nach Art. 57 Abs. 1 lit. p DSGVO abzufassenden und zu veröffentlichenden Kriterien für die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Art. 41 DSGVO und einer Zertifizierungsstelle gemäß Art. 43 DSGVO die Kundmachung einer Verordnung vor.

Art. 57 Abs. 4 DSGVO sieht im Fall von offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anfragen die Möglichkeit vor, dass die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern kann, aufgrund der Anfrage tätig zu werden. Die Datenschutzbehörde kann für exzessive, offensichtlich schikanöse Anfragen eine Gebühr in der Relation zu den ihr tatsächlich entstandenen Kosten verlangen.

Nachdem Art. 57 Abs. 1 lit. v DSGVO als Aufgabe auch die Erfüllung jeder sonstigen Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten vorsieht, erscheint – in dem von lit. v vorgesehenen Bereich – eine Konkretisierung von Aufgaben der Datenschutzbehörde zulässig.

Zu § 11:

Die Befugnisse der Aufsichtsbehörde werden in Art. 58 DSGVO festgelegt und sind weitgehend nicht durchführungsbedürftig. Jedoch bedarf es weiterer Konkretisierungen insbesondere hinsichtlich der Überprüfung von Datenverarbeitungen und des Einschau- bzw. Betretungsrechts. Dies soll in den Abs. 1 und 2 unter Anlehnung an die bisherigen Regelungen in § 30 Abs. 2 und 4 DSG 2000 vorgesehen werden.

Mit Abs. 2 soll Art. 58 Abs. 1 lit. f DSGVO durchgeführt werden, da dieser auf das „Verfahrensrecht des Mitgliedstaats“ verweist. Inhaltlich sind diese Bestimmungen auch in § 30 DSG 2000 vorgesehen.

Erforderlich erscheint zudem die Festlegung einer – zum Teil auf dem bisherigen § 30 Abs. 5 DSG 2000 basierenden – Verschwiegenheitsregelung für Informationen, die der Datenschutzbehörde oder ihren Beauftragten bei der Kontrolltätigkeit zukommen; dies soll in Abs. 3 geregelt werden. Informationen, die der Datenschutzbehörde oder den von ihr Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Für das Strafverfahren stellt § 76 Abs. 2 StPO das Verhältnis zwischen Amtshilfe und Verschwiegenheitspflichten insofern klar, als Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, die sich auf Straftaten bestimmter Personen beziehen, grundsätzlich ohne Rücksicht auf bestehende Verschwiegenheitspflichten zu beantworten sind. Nach dem Willen des Gesetzgebers wird damit ein Vorrang strafgerichtlicher Erhebungsersuchen vor der Amtsverschwiegenheit statuiert (*Lendl* in *Fuchs/Ratz*, WK StPO § 76 Rz 30) und auch Ersuchen, die sich auf automationsunterstützt verarbeitete personenbezogene Daten erstrecken, dürfen nicht bloß mit dem Hinweis auf die besondere Qualität der Datenermittlung und -verarbeitung abgelehnt werden.

Ebenfalls aus dem DSG 2000 (§ 30 Abs. 6a) übernommen werden soll in Abs. 4 die Möglichkeit bei Gefahr im Verzug, die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51, untersagen zu können.

Die in Art. 58 Abs. 3 lit. b DSGVO geregelte Befugnis, von sich aus oder auf Anfrage Fragen an bestimmte Einrichtungen richten zu können, gilt bereits unmittelbar.

Nach Art. 58 Abs. 5 DSGVO hat jeder Mitgliedstaat durch Rechtsvorschriften vorzusehen, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen. In Abs. 3 soll unter anderem diese Vorgabe durchgeführt werden.

Der Datenschutzbehörde obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen. Auf die Verhängung solcher Geldbußen (Art. 83 DSGVO) findet das Verwaltungsstrafgesetz 1991 (VStG), BGBl. Nr. 52/1991, insoweit Anwendung, als die DSGVO im Rahmen des Anwendungsvorranges nicht speziellere Regelungen vorsieht (siehe zB die Regelung zum Kumulierungsverbot gemäß Art. 83 Abs. 3 DSGVO).

Unter den von der DSGVO vorgesehenen Voraussetzungen (Art. 83 iVm Erwägungsgrund 148 der DSGVO) bzw. nach dem VStG kann auch eine Verwarnung erteilt bzw. eine Ermahnung ausgesprochen werden.

Art. 58 Abs. 6 DSGVO, welcher die Möglichkeit bietet, dass jeder Mitgliedstaat durch Rechtsvorschriften vorsehen kann, dass seine Aufsichtsbehörde neben den in den Art. 58 Abs. 1, 2 und 3 DSGVO aufgeführten Befugnissen über zusätzliche Befugnisse verfügt, wird nicht in das DSG übernommen, da diese Rechtsvorschriften gegebenenfalls jeweils mit der zugehörigen Materie geregelt werden müssen. Die Ausübung dieser Befugnisse darf jedoch dabei nicht die effektive Durchführung des Kapitels VII der DSGVO beeinträchtigen.

Zu § 12:

Die Verpflichtung zur Erstellung eines Tätigkeitsberichtes ergibt sich bereits grundsätzlich aus Art. 59 DSGVO. Jedoch erscheint es erforderlich zu konkretisieren, dass die Datenschutzbehörde bis zum 31. März eines jeden Jahres einen den Vorgaben des Art. 59 DSGVO entsprechenden Tätigkeitsbericht zu erstellen und vorzulegen hat. Damit wird grundsätzlich die Regelung des § 37 Abs. 5 DSG 2000 übernommen.

Im Zusammenhang mit der Vorlage des Tätigkeitsberichtes soll auch weiterhin – wie bereits in § 37 Abs. 6 DSG 2000 vorgesehen – die Datenschutzbehörde verpflichtet sein, Entscheidungen von grundsätzlicher Bedeutung für die Allgemeinheit unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

Zu § 13:

Die in Kapitel VIII der DSGVO (Rechtsbehelfe, Haftung und Sanktionen) enthaltenen Regelungen erfordern zum besseren Verständnis – zumindest zum Teil – eine Durchführung ins nationale Recht. Dies betrifft in erster Linie die Art. 77 bis 79 DSGVO, die die Beschwerde und die Rechtsbehelfe regeln. Keiner Durchführung ins nationale Recht bedürfen hingegen etwa Art. 81 und zum Teil auch Art. 83 DSGVO.

In § 13 sollen im Rahmen der Durchführung des Art. 77 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde sowie die Grundsätze des Verfahrens vor der Aufsichtsbehörde geregelt werden. Diesbezüglich werden die bereits in § 31 Abs. 3, 4, 7 und 8 DSG 2000 vorgesehenen Regelungen zum Teil übernommen.

Die Datenschutzbehörde hat im Falle einer Beschwerde auf Ersuchen der betroffenen Person weitere Unterstützung zu leisten. Diese Unterstützung entspricht inhaltlich und umfänglich der gemäß § 13 Abs. 3 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBl. Nr. 51/1991, zu leistenden Manuduktionspflicht.

Abs. 7 soll die Vorgaben zur Unterrichtungspflicht der Datenschutzbehörde gegenüber dem Beschwerdeführer im Rahmen des Art. 77 Abs. 2 DSGVO durchführen.

Abs. 8 soll Detailregelungen zu Art. 78 Abs. 2 DSGVO schaffen.

Im Übrigen soll die Datenschutzbehörde gemäß Abs. 10 auch ausdrücklich die Möglichkeit bekommen, Amtssachverständige im Verfahren beiziehen zu können.

Abs. 10 orientiert sich hinsichtlich der Entscheidungsfristen gemäß § 73 AVG an der Regelung in § 8 Abs. 2 Z 1 des Verwaltungsgerichtsverfahrensgesetzes (VwGVG), BGBl. I Nr. 33/2013. Im Fall der

Datenschutzbehörde soll auch während eines Verfahrens nach Art. 56 und 60 DSGVO die Entscheidungsfrist gehemmt werden. Dies betrifft insbesondere die Verfahren der federführenden Aufsichtsbehörde im Fall des Vorliegens eines sog. „Lokalen Falles“ gemäß Art. 56 Abs. 2 ff DSGVO sowie die Verfahren im Rahmen der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden gemäß Art. 60 DSGVO und den Fall des Kohärenzverfahrens gemäß Art. 63 DSGVO.

Zu § 14:

Mit § 14 sollten weitere verfahrensrechtliche Regelungen im Verfahren vor der Datenschutzbehörde festgelegt werden.

In diesem Sinne werden die Regelungen des bisherigen § 31a Abs. 2 bis 4 DSG 2000 zum Teil in die Abs. 1 und 2 übernommen und entsprechend angepasst. Inhaltlich teilweise übernommen werden soll auch § 34 Abs. 1 und 2 DSG 2000.

Abs. 4 soll auf der Basis der bisherigen Regelungen in § 38 DSG 2000 die Bescheide der Datenschutzbehörde näher regeln. Dazu ist anzumerken, dass von dieser Bestimmung – wie bisher im DSG 2000 – die Überlassung von personenbezogenen Daten (an Auftragsverarbeiter) ins Ausland erfasst sein soll. Das „Überlassen“ soll in der Gesetzesbestimmung jedoch nicht mehr ausdrücklich erwähnt werden, da der DSGVO dieser Begriff fremd ist.

Zu § 15:

§ 15 regelt die Parteistellung und Rechtsmittellegitimation der Verantwortlichen des öffentlichen Bereichs. Die Definition des Verantwortlichen des öffentlichen Bereichs ist an § 5 Abs. 4 DSG 2000 angelehnt. Zu den Verantwortlichen des öffentlichen Bereichs zählen sohin etwa der Bund, die Länder, die Gemeinden, die Kammern und Sozialversicherungsträger sowie die anerkannten Kirchen und Religionsgemeinschaften.

Zu § 16:

§ 16 soll den Rechtsmittelzug von der Datenschutzbehörde zum Bundesverwaltungsgericht regeln und übernimmt dabei weitgehend die bereits bestehenden Regelungen in § 39 DSG 2000 zum Verfahren vor dem Bundesverwaltungsgericht.

Zu § 17:

Mit § 17 sollen die Vorgaben des Art. 80 Abs. 1 DSGVO durchgeführt werden. Dies erscheint insbesondere erforderlich, um auf die vorstehenden verfahrensrechtlichen Bestimmungen im DSG verweisen zu können.

Zu § 18:

§ 18 sieht erforderliche Konkretisierungen zu der in Art. 82 DSGVO geregelten Haftung und dem Recht auf Schadenersatz vor. Dabei wird – neben dem allgemeinen Anspruch auf Schadenersatz in Abs. 1 – das für Klagen zuständige Gericht in Abs. 2 festgelegt.

Zu § 19:

Art. 83 DSGVO regelt die Verhängung von Geldbußen und gilt grundsätzlich unmittelbar. Bereits in der DSGVO ist grundgelegt, dass die Geldbußen von der Datenschutzbehörde verhängt werden sollen. Erforderlich erscheint eine Regelung, unter welchen Voraussetzungen Geldbußen gegen juristische Personen verhängt werden können, wem die verhängten Geldbußen zufließen sollen und wie die Vollstreckung der Geldbußen vorgenommen werden soll.

Die Verhängung von Geldbußen gegen juristische Personen orientiert sich an der geltenden Regelung des § 99d des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993.

Art. 83 Abs. 7 DSGVO sieht vor, dass unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Art. 58 Abs. 2 DSGVO jeder Mitgliedstaat Vorschriften dafür festlegen kann, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können. Nachdem im österreichischen Recht Geldbußen gegen Behörden und öffentliche Stellen grundsätzlich nicht vorgesehen sind, soll in Abs. 5 von dieser Ausnahmemöglichkeit Gebrauch gemacht werden.

Zu § 20:

Die Regelungen zum Datenschutzrat sollen aus dem DSG 2000 großteils übernommen und an die geänderten Vorgaben angepasst bzw. ergänzt werden. Zur Erfüllung seiner Aufgaben kann der Datenschutzrat Empfehlungen in datenschutzrechtlicher Hinsicht an die Bundesregierung und die

Bundesminister richten; dies umfasst – unter Beachtung des unmittelbar anwendbaren Unionsrechts – auch Empfehlungen zu unionsrechtlichen Regelungsvorhaben.

Zu § 21:

Die Regelungen zum Datenschutzrat sehen im DSG 2000 eine partielle Erneuerung des Datenschutzrates nach der Wahl des Hauptausschusses des Nationalrates vor, wodurch für die Bestellung von Mitgliedern bzw. Ersatzmitgliedern – abhängig von der entsendenden Stelle – uneinheitliche Regelungen bestehen.

Aufgrund dessen soll nun eine einheitliche Funktionsperiode für die Mitglieder und Ersatzmitglieder des Datenschutzrates festgelegt werden, welche an die Neuwahl des Hauptausschusses des Nationalrates anknüpft. Geregelt werden soll insbesondere auch die Beendigung der Funktion der Mitglieder und Ersatzmitglieder des Datenschutzrates. Dabei soll klargestellt werden, dass das Mitglied oder Ersatzmitglied auch von sich aus die Funktion vorzeitig zurücklegen kann. Nach der Bekanntgabe des freiwilligen Ausscheidens durch das Mitglied oder Ersatzmitglied hat die entsendende Stelle ehestmöglich ein neues Mitglied oder Ersatzmitglied zu nominieren.

Mitglieder und Ersatzmitglieder des Datenschutzrates, die außerhalb von Wien wohnen, sollen im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der angemessenen Reisekosten nach Maßgabe der Reisegebührenvorschriften des Bundes haben. Die veraltete Bezugnahme auf die Gebührenstufe 3 im geltenden § 42 Abs. 6 DSG 2000 soll entfallen. Reisegebühren sind jedoch nicht zu vergüten, wenn eine Sitzung noch nicht avisiert worden ist. Nach Avisierung einer Sitzung sind allenfalls anfallende Stornogebühren in der nachgewiesenen Höhe zu ersetzen. Weder Reise- noch Stornogebühren können Ersatzmitglieder geltend machen, wenn das zugehörige Mitglied an der Sitzung teilnimmt.

Zu § 22:

Die Wahl des Vorsitzenden und der stellvertretenden Vorsitzenden soll ausführlicher festgelegt werden. So sollen Wahlvorschläge von den Mitgliedern bereits mit der Einladung zur konstituierenden Sitzung an die Mitglieder und Ersatzmitglieder übermittelt werden und allfällig notwendige Stichwahlen zulässig sein. Die Regelungen für die Wahl des Vorsitzenden und der stellvertretenden Vorsitzenden finden sinngemäß auch im Fall einer vorzeitigen Beendigung der Funktion des Vorsitzenden oder eines stellvertretenden Vorsitzenden Anwendung. In diesem Fall soll keine konstituierende Sitzung stattfinden.

Der Vorsitzende vertritt den Datenschutzrat nach außen. Insbesondere kann er die Öffentlichkeit über die Ergebnisse der Sitzungen des Datenschutzrates informieren. Einer der stellvertretenden Vorsitzenden vertritt den Vorsitzenden bei dessen Verhinderung. Im Falle der Beendigung der Funktion des Vorsitzenden vor Ablauf seiner Funktionsperiode, hat einer der stellvertretenden Vorsitzenden die Wahl eines Vorsitzenden umgehend in die Wege zu leiten. Gleiches gilt für den Vorsitzenden, wenn die Funktion eines stellvertretenden Vorsitzenden vor Ablauf seiner Funktionsperiode endet. Abs. 2 gilt sinngemäß.

Zu § 23:

§ 23 regelt die Einberufung der Sitzungen und die Form der Beschlussfassung sowie die Möglichkeit, Arbeitsausschüsse zu bilden sowie Sachverständige beizuziehen.

Zu § 24:

Die Regelungen betreffend die Verschwiegenheit über alle ausschließlich aus der Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen finden sowohl auf ordentliche als auch außerordentliche Sitzungen (Präsidium) des Datenschutzrates sowie auf Sitzungen der Arbeitsausschüsse Anwendung und umfassen insbesondere auch vorbereitende Unterlagen. Durchbrochen ist diese Geheimhaltungsregelung durch die Möglichkeit des Vorsitzenden, im Rahmen seiner Funktion, in der er den Datenschutzrat nach außen vertritt, die Öffentlichkeit über Ergebnisse der Sitzungen des Datenschutzrates zu informieren.

Zu § 25:

Art. 6 Abs. 2 DSGVO sieht vor, dass die Mitgliedstaaten „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen (können), 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.“ Diese sogenannte „Flexibilisierungsklausel“ ermöglicht den Mitgliedstaaten somit trotz Vorliegens einer Unionsverordnung, die in den Grenzen des Anwendungsbereichs des Unionsrechts grundsätzlich auf den öffentlichen und privaten Bereich gleichermaßen anwendbar ist, auf nationaler Ebene (neben Art. 6 Abs. 3, Art. 23 und Kapitel IX der DSGVO) bestimmte „spezifischere Bestimmungen“ zu erlassen. Wenngleich diese Klausel im Verhandlungsprozess – unter Hinweis auf die Besonderheiten des öffentlichen Sektors mit seinen stark

ausdifferenzierten bereichsspezifischen Regelungen und der daraus resultierenden Notwendigkeit einer verbleibenden mitgliedstaatlichen Regelungsbefugnis – zunächst nur auf den öffentlichen Sektor gerichtet war, wird sie auch auf den privaten Sektor zu erstrecken sein. In Fällen, in denen den Mitgliedstaaten etwa aus Art. 8 EMRK und der darauf basierenden EGMR-Judikatur aktive Schutzpflichten für die betroffene Person als Grundrechtsträger erwachsen, wird dies sogar geboten sein. Auch der Juristische Dienst des Rates hat in der Sitzung des Ausschusses der Ständigen Vertreter am 26. November 2014 betont, dass in Zusammenschau von Art. 1 Abs. 2a (der damaligen Textfassung; nunmehr Art. 6 Abs. 2 DSGVO) und Art. 6 Abs. 3 im Lichte der ergänzend aufgenommenen Ausführungen in Erwägungsgrund 8 (der damaligen Textfassung; entspricht nunmehr Erwägungsgrund 10) die Mitgliedstaaten befugt sind, auch spezifischere Vorschriften zum Schutz Privater beizubehalten oder zu erlassen. Zudem ist auch auf den Erwägungsgrund 45 hinzuweisen, wonach unter den dort genannten Voraussetzungen auch Regelungen zu natürlichen Personen (als Verantwortliche) getroffen werden können.

§ 25 soll nicht zur Anwendung kommen, wenn materiengesetzliche Regelungen (zB im Bundesstatistikgesetz, BGBl. I Nr. 163/1999, oder in § 219 Abs. 4 der Zivilprozessordnung (ZPO), RGBl. Nr. 113/1895) die Verarbeitung von Daten zum Zweck der wissenschaftlichen Forschung und Statistik vorsehen. Diese Regelungen sollen daher leges speciales zu den allgemeinen Regelungen des § 25 darstellen und diesem vorgehen.

„Wissenschaftliche Forschung“ soll – wie auch schon nach den Erläuterungen zu § 46 DSG 2000 – nicht einen inhaltlich abgegrenzten Bereich bezeichnen – etwa in der Richtung, dass nur Grundlagenforschung erfasst und angewandte Forschung ausgeschlossen wäre –, sondern als Bereich verstanden werden, in dem eine bestimmte Methode der Vorgangsweise, nämlich eine „wissenschaftliche“, angewendet wird. Wissenschaftliche Forschung im oben genannte Sinn kann durch Verantwortliche des öffentlichen oder des privaten Bereichs vorgenommen werden.

Der Begriff „Statistik“ wird dahingehend verstanden, dass es sich um methodologisch „wissenschaftliche Statistik“ handelt, da nur unter dieser Voraussetzung eine Privilegierung sachlich zu rechtfertigen ist. Abgesehen davon soll aber dieser Begriff sowohl die sogenannte „amtliche Statistik“ als auch sonstige (mit wissenschaftlichen Methoden durchgeführte) Statistik umfassen.

Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist. Dies kann insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) geboten sein.

Zu § 26:

Die Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen soll unter diesen Voraussetzungen in § 26 geregelt werden, wobei die bereits im DSG 2000 bestehenden Regelungen weitgehend übernommen werden sollen. In der Vergangenheit ergaben sich Fragstellungen hinsichtlich der Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen vor allem im Hinblick auf die sog. Geburtstagsgratulationen. Die Verarbeitung von personenbezogenen Daten aus dem Zentralen Melderegister für Geburtstagsgratulationen richtet sich jedoch grundsätzlich nach den Vorgaben im Meldegesetz 1991 (MeldeG), BGBl. Nr. 9/1992.

Auch hier gilt, dass die Datenschutzbehörde die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen hat, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist. Dies kann insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) geboten sein.

Zu § 27:

Die in § 48 DSG 2000 geregelte publizistische Tätigkeit umfasst derzeit nur Medienunternehmen, Mediendienste oder ihre Mitarbeiter und findet auf Verarbeitungen zu künstlerischen Zwecken grundsätzlich keine Anwendung. Nachdem Art. 85 DSGVO nicht darauf abstellt, dass es sich um ein Unternehmen handelt, soll diese Einschränkung entsprechend beseitigt werden. Weiters sollen nun auch Verarbeitungen zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfasst werden, wie es auch in Art. 85 DSGVO vorgesehen ist. Die vorgeschlagene Regelung stellt damit nicht mehr darauf ab, wer die personenbezogenen Daten verarbeitet bzw. ob die Verarbeitung durch ein Unternehmen vorgenommen wird, sondern nur darauf, zu welchen Zwecken diese erfolgt.

Hinsichtlich der Anwendbarkeit der datenschutzrechtlichen Regelungen für Verarbeitungen zu derartigen Zwecken sollen im Rahmen der Vorgaben des Art. 85 DSGVO entsprechende Ausnahmen geschaffen werden. Anwendbar bleiben jedoch die Vorgaben der DSGVO zu den Grundsätzen für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO), zum Auftragsverarbeiter (Art. 28 und 29 DSGVO), zur

Sicherheit der Verarbeitung (Art. 32 DSGVO) sowie allgemein jene Kapitel der DSGVO, von denen Art. 85 DSGVO keine Ausnahmen vorsieht. Inhaltlich sollen damit weitgehend die von Art. 48 DSG 2000 vorgesehenen Ausnahmen für derartige Verarbeitungen erhalten bleiben.

Von den Bestimmungen dieses Bundesgesetzes ist nur § 6 (Datengeheimnis) anzuwenden; davon unberührt bleibt die Anwendung des verfassungsrechtlich verankerten Grundrechts auf Datenschutz gemäß § 1.

Für Verarbeitungen, die dem Mediengesetz (MedienG), BGBl. Nr. 314/1981, unterliegen, gelten die Vorschriften des MedienG auch ohne ausdrückliche Anordnung.

Zu § 28:

§ 28 soll im Rahmen des Art. 6 Abs. 2 und 3 sowie Art. 23 DSGVO und Kapitel IX der DSGVO iVm Erwägungsgrund 10 die bisher in § 48a DSG 2000 geregelte Verwendung von personenbezogenen Daten im Katastrophenfall regeln. Dabei werden die Grundsätze der bereits bestehenden Regelung übernommen und entsprechend den neuen Erfordernissen der DSGVO angepasst.

Art. 49 Abs. 1 lit. d DSGVO erlaubt eine Übermittlung ins Ausland, wenn dies aus wichtigen Gründen des öffentlichen Interesses notwendig ist. Darunter fällt jedenfalls auch ein entsprechend schwerwiegender Katastrophenfall (zB Lawinen, Vulkanausbrüche, Erdbeben, Tsunami).

Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann. Zu den Hilfsorganisationen zählen beispielsweise die Caritas Österreich, der Arbeiter-Samariter-Bund Österreichs oder das Österreichische Rote Kreuz. Weiters werden am Ort der Katastrophe tätige nationale und internationale Hilfsorganisationen einzubeziehen sein.

Zu § 29:

Nachdem weder das DSG 2000 – noch zuvor das DSG 1978 – eine systematische Regelung des Beschäftigtendatenschutz enthalten hat, sondern sich derartige Regelungen in arbeitsrechtlichen Vorschriften (zB im Arbeitsverfassungsgesetz (ArbVG), BGBl. Nr. 22/1974) finden, wird von einer inhaltlich Ausgestaltung des Beschäftigtendatenschutzes im neuen DSG Abstand genommen. Fortgeschrieben werden soll jedoch das bestehende Verhältnis zwischen dem DSG 2000 (§ 9 Z 11 DSG 2000) und dem ArbVG (siehe etwa OGH 17.9.2014, 6 Ob A1/14m). Inhaltliche Regelungen zum Datenschutz im Beschäftigungskontext können unmittelbar auf Art. 88 DSGVO gestützt und in diesem Rahmen in den betreffenden arbeitsrechtlichen Materiengesetzen geregelt werden. Eine diesbezügliche Notifikation an die Europäische Kommission nach Art. 88 Abs. 3 DSGVO ist erforderlich. Den bestehenden Mitwirkungsrechten der Belegschaft wird nicht derogiert.

Zu den §§ 30 bis 33:

Der mit der DSG-Novelle 2010 in das DSG 2000 eingefügte 9a. Abschnitt sah in den §§ 50a ff ausführliche Regelungen für die Videoüberwachung vor. Viele der aufgrund der technischen Fortentwicklung auf diesem Gebiet entwickelten und nunmehr in der Praxis verbreiteten Videoanwendungen wie Action-Cams, Wildkameras sowie weitere Videoanwendungen im Freizeitbereich fielen jedoch definitionsgemäß nicht in den Anwendungsbereich des 9a. Abschnittes. Diese Anwendungen konnten nicht zweifelsfrei auf den § 50a DSG 2000 gestützt werden, sondern unterlagen den allgemeinen Vorschriften der §§ 6 ff DSG 2000.

Einige der im 9a. Abschnitt enthaltenen Sonderregelungen für Videoüberwachungen haben sich in der Praxis nicht bewährt und sollen daher nicht beibehalten werden. So wurde etwa das Hinterlegen des Schlüssels zur Videoüberwachung bei der Datenschutzbehörde nach § 50c Abs. 1 DSG 2000 in der Praxis nicht eingeführt. Ferner erscheint eine Unterscheidung zwischen einer digitalen und einer analogen Aufzeichnung nach § 50c Abs. 2 DSG 2000 nicht mehr zweckmäßig. Das von § 50e DSG 2000 – in Abweichung vom § 26 Abs. 1 DSG 2000 – vorgesehene Auskunftsrecht hat sich in der Praxis als zum Teil undurchführbar erwiesen, da es eine Sichtung der Videoaufnahmen über den Auskunftswerber hinaus von anderen Personen voraussetzte, in deren Rechte dadurch eingegriffen wurde.

Bewährt hat sich hingegen generell, dass die Videoüberwachung im DSG 2000 als besondere Datenverarbeitung geregelt wird und an die potentiellen Gefahren angepasste Voraussetzungen für den Einsatz dieser Technologie vorgegeben werden. So hat sich vor allem das Verbot der Videoüberwachung für den höchstpersönlichen Lebensbereich einer betroffenen Person sowie das Verbot des Einsatzes der Videoüberwachung zum Zweck der Mitarbeiterkontrolle bewährt. Gleiches ist hinsichtlich des Verbots des automationsunterstützten Abgleiches mit anderen Bilddaten und sensiblen Daten anzumerken. Bewährt hat sich überdies auch die Protokollierungs- und Kennzeichnungspflicht.

Aufgrund dieser Erfahrungen sollen im Rahmen des Art. 6 Abs. 2 und 3 sowie Art. 23 DSGVO und Kapitel IX der DSGVO iVm Erwägungsgrund 10 auch im DSG Bildaufnahmen gesondert geregelt werden.

Die neue Regelung zielt darauf ab, grundsätzlich alle Bildaufnahmen durch Verantwortliche des privaten Bereichs (so zB auch das Anfertigen von Fotografien zu beruflichen Zwecken) diesen Bestimmungen unterliegen zu lassen, sofern diese nicht ohnehin aufgrund von Art. 2 Abs. 2 lit. c DSGVO („Haushaltsausnahme“) vom Anwendungsbereich ausgenommen sind und auch nicht andere Gesetze hierzu Besonderes vorsehen. Davon umfasst sind auch Aufnahmen im Rahmen der Privatwirtschaftsverwaltung (zB Überwachung von öffentlichen Gebäuden, soweit diese im Rahmen der Privatwirtschaftsverwaltung erfolgt). Aufnahmen zur Vollziehung hoheitlicher oder schlicht hoheitlicher Aufgaben sollen hingegen nicht von diesem Abschnitt erfasst sein; diese benötigen weiterhin eine gesonderte gesetzliche Rechtsgrundlage (§ 1 DSG und Art. 18 B-VG).

Zudem soll auch die mit der Videoaufzeichnung allenfalls verbundene Tonaufnahme von diesem Abschnitt erfasst sein.

Der Begriff „Ereignis“ soll dabei weit verstanden werden. Insbesondere soll auch eine mobile Videoaufzeichnung (zB das Filmen einer Abfahrt mit einer Action-Cam) erfasst sein. In diesem Sinne soll auch der Begriff „Bildaufnahme“ weit ausgelegt werden und auch bloße Aufzeichnungen erfassen, die zwar ein bestimmtes Objekt oder eine bestimmte Person zum Inhalt haben, aber nicht auf eine „Überwachung“ abzielen.

Für den Einsatz einer Bildaufnahme und die Verarbeitung der Aufnahmen gilt der Verhältnismäßigkeitsgrundsatz. Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.

Hinsichtlich der Voraussetzungen soll zwischen dem ersten Schritt des bloßen Einsatzes einer Bildaufnahme (dies umfasst die Verarbeitung mit Ausnahme der Übermittlung) und dem – mit einem weiteren Eingriff verbundenen – zweiten Schritt des Übermittelns einer Aufnahme unterschieden werden. In beiden Fällen sollen die Voraussetzungen, unter welchen diese Technik für private Zwecke eingesetzt werden darf, abschließend geregelt werden.

§ 30 Abs. 2 listet allgemeine Tatbestände auf, bei deren Vorliegen die Bildverarbeitung zulässig sein soll. Im Sinne der nötigen Flexibilität in der Praxis sieht § 30 Abs. 2 Z 4 als einen Erlaubnistatbestand das Vorliegen überwiegender berechtigter Interessen des Verantwortlichen oder eines Dritten im Einzelfall vor.

Von Z 4 soll auch der Fall der Überwachung eines bestimmten Objekts oder einer bestimmten Person erfasst sein, zu dessen oder deren Schutz der Einsatz technischer Einrichtungen zur Bildverarbeitung erforderlich ist und unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Unionsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Verantwortlichen spezielle Sorgfaltspflichten zum Schutz des aufgenommenen Objekts oder der aufgenommenen Person auferlegen.

In den in § 30 Abs. 3 geregelten Fällen wird die Interessenabwägung (vgl. § 30 Abs. 2 Z 4) bereits auf gesetzlicher Ebene vorgenommen. Abgebildet werden exemplarische, quasi massenhaft auftretende Fallkonstellationen wie zB die Überwachung von Einfamilienhäusern (Z 1), die Überwachung in öffentlichen Verkehrsmitteln (Z 2) oder sog. Freizeitkameras uÄ. (Z 3). Zugleich wird der Vollzugspraxis ausdrücklich die Grundlage für mögliche Analogien eröffnet. Damit sollen zukünftige, heute noch nicht absehbare technologische Entwicklungen handhabbar werden. Zu Z 3 ist ergänzend zu bemerken, dass diese Bestimmung keine Grundlage für eine anlasslose Dokumentation personenbezogener Daten im Anwendungsbereich der § 30 zwecks potenzieller Heranziehung als Beweismittel in Rechtsstreitigkeiten bilden soll.

Bei Vorliegen von Nutzungsrechten an der Liegenschaft setzt die Zulässigkeit einer Bildaufnahme nach Abs. 3 Z 1 die Einwilligung aller betroffenen zusätzlichen Nutzungsberechtigten voraus. Dies ergibt sich bereits aus Abs. 2 Z 2.

Von Abs. 3 Z 2 sollen insbesondere auch die derzeit in der Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004, enthaltenen Videoüberwachungen (Standardanwendung „SA032 Videoüberwachung“, zB für Trafiken) sowie auch die Bildaufnahmen in öffentlichen Verkehrsmitteln (zB Wiener Linien) erfasst sein.

Die Verarbeitung akustischer Informationen ist im Einzelfall zu beurteilen; in den Fällen des Abs. 3 Z 1 und 2 wird dies nicht zulässig sein.

Mit „Objekten“ nach § 30 Abs. 3 Z 3 sind etwa KFZ-Kennzeichen oder Fahrzeugaufschriften gemeint.

Bildaufnahmen, mit denen in den höchstpersönlichen Lebensbereich einer betroffenen Person eingegriffen wird, sollen ausschließlich mit ausdrücklicher Einwilligung zulässig sein. Damit sollen etwa

auch kommerzielle Filmaufnahmen ermöglicht werden. Abgesehen vom Kernbereich der Privatsphäre (§ 31 Abs. 4 Z 1) soll auch ein unverhältnismäßiger Eingriff in deren Vorfeld unzulässig sein. Zu denken ist hier etwa an die Kontrolle von Zugängen zu Räumlichkeiten, in denen typischerweise höchstpersönliche Verhaltensweisen verwirklicht werden (zB medizinische Einrichtungen, Sakralräume, Hygieneräume). Erweisen sich solche Zutrittskontrollen jedoch im Einzelfall als für die Wahrung überwiegender Interessen als erforderlich und sind sie verhältnismäßig ausgestaltet, liegt kein Fall des § 31 Abs. 4 Z 1 vor.

Der Einsatz von Bildaufnahmen zur Mitarbeiterkontrolle soll weiterhin gänzlich untersagt werden. Die Unzulässigkeit der Auswertung umfasst auch die Durchsuchung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

§ 31 stellt klar, dass die Zulässigkeit der Übermittlung von Bildaufnahmen davon abhängig gemacht wird, dass erstens die Daten zulässigerweise nach § 30 ermittelt worden sind und zweitens einer der Fälle des § 30 Abs. 2 vorliegen muss. Der Umfang der zu übermittelnden Daten ist im Einzelfall anhand der Verhältnismäßigkeit zu beurteilen. Das Übermitteln iSd § 31 soll insbesondere die Veröffentlichung von Aufnahmen oder die Zugänglichmachung mittels eines Dienstes der Informationsgesellschaft (zB in sozialen Netzwerken im Internet) umfassen. Diesfalls ist im Einzelfall die Zulässigkeit einer solchen Übermittlung (zB Daten nach § 30 Abs. 3 Z 3) anhand der Kriterien des § 30 Abs. 2 Z 2 und 4 zu beurteilen bzw. die Erforderlichkeit von Maßnahmen zum Ausschluss der Identifizierbarkeit der betroffenen Personen mit anderen Mitteln (zB „Verpixeln“) abzuwägen. In diesem Zusammenhang ist bei der Abwägung das Prinzip „Privacy by design“ zu berücksichtigen.

Im Wege einer Bildaufnahme ermittelte personenbezogene Daten dürfen im Rahmen der Vorgaben des § 31 auch an eine zuständige Behörde oder das zuständige Gericht übermittelt werden, wenn beim Verantwortlichen der begründete Verdacht entstanden ist, die personenbezogenen Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Verantwortlichen bleiben unberührt. Eine zuständige Behörde kann insbesondere die Staatsanwaltschaft, die Finanzmarktaufsicht oder die Datenschutzbehörde sein.

Die Protokollierungspflicht soll wie bisher beibehalten werden und um besondere Datensicherheitsmaßnahmen ergänzt werden.

Im Rahmen einer flexibleren Regelung soll sich die Löschungspflicht am jeweiligen Zweck der Bildaufnahme orientieren. Gleichzeitig soll klar zu Ausdruck gebracht werden, dass eine länger als 72 Stunden dauernde Speicherung nicht generell zulässig ist.

Beibehalten werden soll grundsätzlich auch die Kennzeichnungspflicht von Bildaufnahmen.

Entfallen soll die bisher bestehende Möglichkeit der Hinterlegung eines Schlüssels bei der Datenschutzbehörde. Nachdem es sich nach den geltenden allgemeinen Datensicherheitsmaßnahmen richtet, ob Bildaufnahmen verschlüsselt werden müssen (und der Schlüssel dann vom Verantwortlichen entsprechend sicher verwahrt werden muss), scheint eine gesonderte Regelung im Abschnitt für die Bildaufnahme nicht erforderlich. Auch gibt es Videoanwendungen, die vergleichsweise geringe Eingriffe nach sich ziehen (zB das Filmen einer Skiabfahrt mit einer Action-Cam), und deshalb mit entsprechend geringeren Datensicherheitsmaßnahmen betrieben werden können, hingegen werden Videoanwendungen, auf denen auch besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) erkannt werden können (zB Videoaufnahmen eines Krankenhauseinganges) höhere Datensicherheitsmaßnahmen und eine Verschlüsselung erfordern.

Ebenfalls entfallen soll die allgemeine Regelung der Auskunft der betroffenen Person. Diese soll sich nach den allgemeinen Regelungen der DSGVO richten. Werden aber entgegen der Vorgaben für die Kennzeichnung gemäß § 33 Abs. 1 keine ausreichenden Informationen bereitgestellt, kann jede von einer Verarbeitung potenziell betroffene Person vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer bezüglichen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

Zu § 34:

Das 3. Hauptstück des DSG regelt die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs. Mit den in diesem

Hauptstück enthaltenen Bestimmungen werden die Kapitel I bis V der Richtlinie (EU) 2016/680 umgesetzt, wobei zur Vermeidung von Wiederholungen und zur Gewährleistungen eines einheitlichen Schutzniveaus soweit wie möglich an die Bestimmungen der DSGVO angeknüpft wird. Die Kapitel VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit) und VIII (Rechtsbehelfe, Haftung und Sanktionen) werden im 3. Hauptstück im 5. Abschnitt umgesetzt.

Die Richtlinie (EU) 2016/680 erlaubt den Mitgliedstaaten ausdrücklich, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden strengere Garantien festzulegen (Art. 1 Abs. 3). Um das bestehende nationale Datenschutzniveau nicht zu senken, werden daher gegebenenfalls bestehende Standards aus dem DSG 2000 übernommen.

§ 34 regelt den Anwendungsbereich des 3. Hauptstücks und setzt die entsprechenden Vorgaben des Art. 1 Abs. 1 und Art. 2 Abs. 1 der Richtlinie (EU) 2016/680 um, erweitert diesen jedoch insoweit, als die Bestimmungen des vorliegenden Hauptstücks auch auf Datenverarbeitungen anzuwenden sind, die nicht in den Anwendungsbereichs des Unionsrechts fallen (und folglich nicht von der Richtlinie (EU) 2016/680 umfasst sind). Dies entspricht dem bisherigen Rechtsbestand, zumal auch das DSG 2000 für den gesamten innerstaatlichen Bereich gilt. Der Begriff „Straftat“ unterliegt als eigenständiger Begriff des Unionsrechts der Auslegung durch den EuGH (vgl. Erwägungsgrund 13 der Richtlinie (EU) 2016/680).

Soweit Strafverfolgungsbehörden auch mit der Erfüllung anderweitiger Aufgaben betraut sind, unterliegen sie in Bezug auf diese Tätigkeiten nicht den Vorschriften des 3. Hauptstücks, sondern der DSGVO (bzw. ergänzenden nationalen Rechtsvorschriften). Hier können sich jedoch – insbesondere im Polizeibereich – zahlreiche Grenzfälle ergeben, etwa wenn zunächst unklar ist, ob eine Datenverarbeitung im Zusammenhang mit einer Straftat steht (zB Fund einer Leiche, wobei noch nicht ersichtlich ist, ob eine Straftat oder aber ein Unfall oder Suizid vorliegt oder Vermisstenmeldung, bei der unklar ist, ob die Person überhaupt gefährdet ist). Derartige Fälle unterliegen den Vorschriften des 3. Hauptstücks (vgl. Erwägungsgrund 12 der Richtlinie (EU) 2016/680). Ebenso erfasst ist die Ausübung hoheitlicher Gewalt durch die Ergreifung von Zwangsmitteln, zB bei Demonstrationen, großen Sportveranstaltungen oder Ausschreitungen (vgl. Erwägungsgrund 12 der Richtlinie (EU) 2016/680). Hingegen unterliegen polizeiliche Verwaltungstätigkeiten, soweit sie nicht in Zusammenhang mit Straftaten stehen, der DSGVO. Dies betrifft etwa die Bereiche Vereins- und Versammlungswesen, Straßenpolizei und Asyl- und Fremdenwesen. Polizeiliche Tätigkeiten zur Abwehr von Gefahren, die nicht in Zusammenhang mit Straftaten stehen, fallen ebenfalls in den Anwendungsbereich der DSGVO (zB Absicherung von Unfallstellen, erste allgemeine Hilfeleistung).

In bestimmten Fällen kann ein polizeilicher Einsatz teils in den Anwendungsbereich der DSGVO, teils in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, etwa wenn zunächst kein Konnex mit einer Straftat besteht, später jedoch ein Einschreiten zur Verhinderung/Verfolgung von Straftaten erforderlich wird (zB Einsatz bei einer Demonstration). Anknüpfungspunkt ist hier der Einsatz von Zwangsmitteln zur Ausübung hoheitlicher Gewalt.

Die Verarbeitung personenbezogener Daten zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken fällt im Regelfall in den Anwendungsbereich der DSGVO; findet die Verarbeitung in diesem Zusammenhang jedoch durch zuständige Behörden zu Zwecken des § 34 statt, so unterliegt sie den Bestimmungen des 3. Hauptstücks (vgl. Art. 4 Abs. 3 der Richtlinie (EU) 2016/680).

Darüber hinaus umfasst der Anwendungsbereich des 3. Hauptstücks auch besondere Datenverarbeitungen des öffentlichen Bereichs. Darunter ist die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärische Eigensicherung zu verstehen. Vom Anwendungsbereich des 3. Hauptstücks sollen etwa auch die nachrichtendienstliche Aufklärung und die Luftraumüberwachung sowie andere Tätigkeiten der Landesverteidigung außerhalb der Verwaltungsverfahren erfasst sein.

Nur die Verarbeitung von Daten zu Zwecken des § 34 durch zuständige Behörden fällt somit in den Anwendungsbereich des 3. Hauptstücks. Gleiches gilt für die Übermittlung von zu Zwecken des § 34 durch zuständige Behörden verarbeiteten Daten an Verantwortliche außerhalb des Anwendungsbereichs des 3. Hauptstücks. Die Verarbeitung durch diese Verantwortlichen richtet sich in der Folge jedoch – im Rahmen der Vorgaben des § 2 – nach der DSGVO und dem 2. Hauptstück.

Die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (leges speciales) gehen – wie auch schon nach der geltenden Rechtslage – den allgemeinen Regelungen des 3. Hauptstücks vor.

Zu § 35:

Die Begriffsbestimmungen wurden aus der Richtlinie (EU) 2016/680 übernommen.

Der Begriff der „zuständigen Behörde“ umfasst die Strafverfolgungsbehörden sowie sonstige Behörden, denen (gegebenenfalls punktuell) die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse gemäß lit. a durch Gesetz übertragen wurde. Da es sich dabei um sog. staatliche Kernaufgaben handelt, die einer Beleihung grundsätzlich nicht zugänglich sind (vgl. VfSlg. 14.473/1996, 16.400/2001), wird das 3. Hauptstück in der Praxis kaum Anwendung auf Private finden. Beim Verantwortlichen (Art. 4 Z 7 DSGVO) kann es sich aufgrund § 34 im Zusammenhang mit dem 3. Hauptstück stets nur um eine zuständige Behörde handeln.

Private, die im Rahmen von Speicher- und Meldepflichten in Bezug auf Daten, die im Geschäftsverkehr entstehen, im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung gesetzlich verpflichtet sind, unterliegen den Vorschriften der DSGVO, zumal ihnen in diesem Zusammenhang keine hoheitlichen Befugnisse zukommen (vgl. auch Erwägungsgrund 11 der Richtlinie (EU) 2016/680). Sind Private im Rahmen von Mitwirkungspflichten zur Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken für Strafverfolgungsbehörden gesetzlich verpflichtet (zB im Rahmen einer Nachrichtenüberwachung gemäß § 134 Z 3 StPO), so gelten sie insofern als Auftragsverarbeiter (Art. 4 Z 8 DSGVO; vgl. auch Erwägungsgrund 11 der Richtlinie (EU) 2016/680).

Da die Richtlinie (EU) 2016/680 einen funktionalen und keinen organisatorischen Ansatz verfolgt, unterliegen auch zuständige Behörden nur insoweit den Vorschriften des 3. Hauptstücks, als die konkrete Datenverarbeitung den in § 34 genannten Zwecken dient (vgl. Erwägungsgrund 12 der Richtlinie (EU) 2016/680).

Zu § 36:

Mit dieser Bestimmung wird Art. 4 Abs. 1 und 4 der Richtlinie (EU) 2016/680 umgesetzt. Die in Art. 4 Abs. 2 und 3 der Richtlinie (EU) 2016/680 enthaltenen Regelungen betreffend die Weiterverarbeitung von personenbezogenen Daten werden aus systematischen Gründen gemeinsam mit Art. 9 der Richtlinie (EU) 2016/680 in § 40 umgesetzt.

Der in Abs. 1 Z 1 verankerte Grundsatz der Verarbeitung nach Treu und Glauben schließt geheime Überwachungsmaßnahmen oder verdeckte Ermittlungen nicht aus; derartige Eingriffe unterliegen jedoch einer entsprechend strengen Verhältnismäßigkeitsprüfung (vgl. Erwägungsgrund 28 der Richtlinie (EU) 2016/680).

Zu § 37:

Mit dieser Bestimmung werden die Art. 6 und 7 der Richtlinie (EU) 2016/680 umgesetzt. Es handelt sich dabei um eine spezifische Regelung für den Strafverfolgungsbereich; die DSGVO enthält keine derartige Regelung.

Abs. 1 Z 1 ist an die Definition des „Beschuldigten“ gemäß § 48 Abs. 1 Z 2 StPO angelehnt. Darüber hinaus soll auch der „Verdächtige“ (§ 48 Abs. 1 Z 1 StPO) und somit „jede Person, gegen die auf Grund eines Anfangsverdachts ermittelt wird“ vom angeführten Betroffenenkreis mitumfasst sein.

Dem verurteilten Straftäter gleichgestellt sind Personen, die in den Maßnahmenvollzug eingewiesen wurden.

Z 2 soll den Bereich des SPG abdecken. Eine Unterscheidung von einer Straftat verdächtigen Personen nach der StPO und dem SPG erscheint aufgrund der unterschiedlichen Anwendungsbereiche dieser Gesetze zweckmäßig.

Zum automatisierten Abruf bereit gehaltene personenbezogene Daten müssen entsprechend laufend vollständig und aktuell gehalten werden. Unter einem „automatisierten Abruf“ gemäß § 37 Abs. 3 ist insbesondere die Abfrage von Datenbanken zu verstehen.

Die Pflichten nach Abs. 5 können je nach Fall sowohl den Empfänger als auch den Übermittler treffen (zB bei unrichtigen Daten).

Zu § 38:

Diese Bestimmung dient der Umsetzung des Art. 8 der Richtlinie (EU) 2016/680 und enthält wesentliche Grundvoraussetzungen für die Verarbeitung personenbezogener Daten, die sich grundlegend von der Regelung in Art. 6 DSGVO unterscheiden. Das Erfordernis einer gesetzlichen Grundlage ergibt sich neben der Richtlinie auch aus Art. 18 B-VG sowie dem Grundrecht auf Datenschutz gemäß § 1.

§ 38 schafft eine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Wahrung lebenswichtiger Interessen einer Person. Eine solche Regelung erscheint schon deshalb geboten, weil Art. 6 Abs. 1 lit. d DSGVO eine entsprechende Rechtsgrundlage für (u.a.) sonstige Behörden enthält und den Strafverfolgungsbehörden in diesem Zusammenhang keine zusätzlichen Einschränkungen auferlegt werden sollen. Die Regelung wird unmittelbar im Rahmen des DSG verankert, da ansonsten

eine entsprechende Bestimmung in jedem Materiengesetz getroffen werden müsste. Die Richtlinie (EU) 2016/680 sieht eine Verarbeitung personenbezogener Daten zur Wahrung lebenswichtiger Interessen explizit nur im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) vor; eine entsprechende Regelung erscheint jedoch auch in Bezug auf andere Datenkategorien erforderlich.

Zu § 39:

Mit dieser Bestimmung wird Art. 10 der Richtlinie (EU) 2016/680 umgesetzt.

Art. 10 der Richtlinie (EU) 2016/680 sieht für die Verarbeitung von besonderen Kategorien personenbezogener Daten (siehe Art. 9 Abs. 1 DSGVO) neben einer gesetzlichen Grundlage auch die Verarbeitung zur Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen Person oder die Verarbeitung von Daten, die die betroffene Person selbst veröffentlicht hat, vor.

§ 39 Z 2 regelt die Verarbeitung von Daten, die die betroffene Person offensichtlich selbst öffentlich gemacht hat. Dies ist nur für einen der in § 34 genannten Zwecke zulässig; überdies muss die Verarbeitung unbedingt erforderlich sein und es müssen wirksame Maßnahmen auf gesetzlicher Ebene zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden. „Öffentlich machen“ setzt einen offensichtlich willentlichen und aktiv gesetzten Schritt der betroffenen Person zur Veröffentlichung, etwa im Internet oder in Zeitungen, voraus. Die bloße Teilnahme am öffentlichen Leben (zB als Angehöriger einer Minderheit oder als Teilnehmer an einer politischen Kundgebung) kann hingegen nicht darunter verstanden werden. Das Erfordernis einer gesetzlichen Grundlage gemäß Art. 18 B-VG bleibt davon unberührt. Von § 39 Z 2 nicht umfasst ist zudem die Weiterverarbeitung (zB das Abgleichen der offensichtlich von der betroffenen Person selbst öffentlich gemachten Daten mit Datenbanken), wofür eine entsprechende gesetzliche Grundlage erforderlich wäre.

Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) zur Wahrung lebenswichtiger Interessen einer Person kann auf die allgemeine Regelung des § 38 gestützt werden.

Zu § 40:

Mit dieser Bestimmung werden Art. 4 Abs. 2 und 3 sowie Art. 9 der Richtlinie (EU) 2016/680 umgesetzt.

Der Begriff der „Weiterverarbeitung“ wird im vorliegenden Kontext bewusst vermieden, weil die Richtlinie (EU) 2016/680 diesbezüglich von einem grundlegend anderen Konzept ausgeht als die DSGVO und diese Konzepte nicht vermischt werden sollten.

In der Richtlinie (EU) 2016/680 sind Regelungen über die Verarbeitung von personenbezogenen Daten zu anderen Zwecken sowie die Übermittlung in mehreren Bestimmungen enthalten. Das komplexe Zusammenspiel zwischen DSGVO und Richtlinie (EU) 2016/680 in Schnittstellenbereichen – etwa wenn personenbezogene Daten aus dem Strafverfolgungskontext für andere Zwecke weiterverarbeitet oder an andere Behörden übermittelt werden sollen – kommt dadurch in der Richtlinie nicht klar zum Ausdruck. Die Regelungen sollen deshalb im Zuge der Umsetzung in einer gemeinsamen Bestimmung zusammengeführt werden. Abs. 1 sieht vor, dass auch die Verarbeitung zu anderen Zwecken gemäß § 34 stets einer eigenen gesetzlichen Grundlage bedarf. Davon umfasst ist jedenfalls auch eine Verarbeitung von personenbezogenen Daten eines Geschäftsfalles für einen anderen Geschäftsfall (zB Austausch von personenbezogenen Daten zwischen mehreren Strafverfahren ohne entsprechende gesetzliche Vorgaben). Abs. 1 findet dabei jedoch nur Anwendung, wenn die Verarbeitung zu einem anderen Zweck innerhalb des Anwendungsbereichs des § 34 erfolgt. Übermittlungen zu einem Zweck außerhalb des Anwendungsbereichs des § 34 sind hingegen nach Abs. 2 zu beurteilen. Die Weiterverarbeitung personenbezogener Daten im Strafverfolgungskontext ist insofern gegenüber der Erstermittlung grundsätzlich nicht privilegiert (es können jedoch materienspezifische Sonderregelungen getroffen werden, zB hinsichtlich der Verwertung von Zufallsfunden). Die Verarbeitung personenbezogener Daten zu Zwecken der Archivierung im öffentlichen Interesse sowie die wissenschaftliche, statistische oder historische Verarbeitung durch zuständige Behörden stellt ebenfalls einen Anwendungsfall des Abs. 1 dar, wenn sie zu Zwecken des § 34 durchgeführt wird (zB Auswertung zu Präventionszwecken). Die Verarbeitung nach dem Abs. 1 umfasst sowohl die Verarbeitung für einen anderen Zweck durch denselben Verantwortlichen sowie einen anderen Verantwortlichen.

Eine Verarbeitung von nach den Bestimmungen dieses Hauptstücks verarbeiteten personenbezogenen Daten zu anderen als den in § 34 genannten Zwecken ist durch denselben Verantwortlichen hingegen dann nur zulässig, soweit dies gesetzlich oder durch unmittelbar anwendbares Unionsrecht (zB DSGVO) vorgesehen ist.

Abs. 2 sieht vor, dass jede Übermittlung von personenbezogenen Daten einer ausdrücklichen gesetzlichen Grundlage bedarf und nur zulässig ist, wenn der Empfänger zur Verarbeitung der personenbezogenen

Daten befugt ist. Die Regelung gilt unabhängig davon, welchen konkreten Rechtsvorschriften der Empfänger unterliegt bzw. zu welchen Zwecken die weitere Verarbeitung erfolgt.

Die Zulässigkeit der Übermittlung von personenbezogenen Daten ist grundsätzlich getrennt von der Zulässigkeit der Verarbeitung zu prüfen. Das Verhältnis zwischen der Zulässigkeit der Übermittlung und der Verarbeitung beim Empfänger stellt sich somit wie folgt dar: Voraussetzung jeder Übermittlung ist die Zulässigkeit der Verarbeitung durch den Empfänger. Umgekehrt berechtigt aber die bloße Tatsache, dass der Empfänger zur Verarbeitung der personenbezogenen Daten berechtigt wäre, eine zuständige Behörde nicht zur Übermittlung der Daten; die Übermittlung muss zudem gesetzlich ausdrücklich vorgesehen sein.

Eine solche Regelung ist unerlässlich, um personenbezogene Daten, die im Strafverfolgungskontext ermittelt wurden, ausreichend zu schützen: So sind den Strafverfolgungsbehörden bestimmte Ermittlungsmaßnahmen, die besonders gravierend in die Rechte der betroffenen Personen eingreifen – insbesondere geheime Überwachungsmaßnahmen – vorbehalten, die weder sonstigen Behörden noch Privaten erlaubt sind. Dass ein Empfänger zur Verarbeitung der personenbezogenen Daten (etwa aufgrund eines überwiegend berechtigten Interesses) dem Grunde nach berechtigt wäre, soll nicht dazu führen, dass solche im Strafverfolgungskontext ermittelten personenbezogenen Daten von der zuständigen Behörde, die die personenbezogenen Daten ursprünglich ermittelt und verarbeitet hat, etwa an Private übermittelt werden dürfen oder sogar müssen, obwohl der Empfänger die für ihre Ermittlung eingesetzten Mittel selbst niemals hätte einsetzen dürfen. Die Entscheidung, ob eine solche Übermittlung mit den Rechten der betroffenen Person vereinbar ist, wird somit dem Gesetzgeber überantwortet. Entsprechende Übermittlungsregelungen sind schon jetzt in zahlreichen Materiengesetzen (zB SPG und StPO) enthalten, sodass sich diesbezüglich kein zusätzlicher Umsetzungsbedarf ergibt.

Zu § 41:

Mit dieser Bestimmung wird Art. 11 der Richtlinie (EU) 2016/680 umgesetzt. Aufgrund des völlig unterschiedlichen Anwendungsbereichs automatischer Entscheidungsfindungen (zB Rasterfahndung) gegenüber der DSGVO erscheint es nicht zweckmäßig, an die – auch systematisch anders platzierte – Bestimmung des Art. 22 DSGVO anzuknüpfen.

Ein Gesetz, das die automatisierte Entscheidungsfindung im Einzelfall erlaubt, muss nach den Vorgaben des Art. 11 Abs. 1 jedenfalls geeignete Garantien für die Rechte und Freiheiten der betroffenen Person, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, vorsehen. Dies ist bei der Erlassung entsprechender materiengesetzlicher Regelungen jedenfalls zu beachten.

Das in Abs. 3 enthaltene Diskriminierungsverbot bezieht sich auf Art. 21 GRC. Zu beachten ist, dass Profiling aufgrund besonderer Datenkategorien (zB im Rahmen einer Fahndung nach einer Person mit einer bestimmten Hautfarbe) nicht grundsätzlich ausgeschlossen ist; untersagt ist lediglich diskriminierendes Profiling, dh. wenn das Abstellen auf das jeweilige Merkmal nicht aus sachlich gerechtfertigten Gründen erfolgt. In Abs. 3 wird die Definition der besonderen Kategorien personenbezogener Daten aus Art. 9 Abs. 1 DSGVO übernommen (siehe auch Art. 10 der Richtlinie (EU) 2016/680).

Zu § 42:

Mit den Abs. 1 bis 7 werden die Art. 12 und 18 der Richtlinie (EU) 2016/680 umgesetzt, mit den Abs. 8 und 9 Art. 17 der Richtlinie (EU) 2016/680. Da die Betroffenenrechte des Kapitels III der Richtlinie (EU) 2016/680 in zahlreichen Punkten andere Regelungen vorsehen als die DSGVO, ist eine weitgehend gesonderte Regelung der Betroffenenrechte unerlässlich. Die Fristen sowie die Möglichkeit zur Fristverlängerung, die Vorgangsweise bei Verzögerung der Antwort sowie insbesondere die grundsätzliche Unentgeltlichkeit wurden entsprechend den Vorgaben des Art. 12 Abs. 3 bis 5 DSGVO ausgestaltet.

Die Form der Übermittlung der Information gemäß Abs. 1 ist grundsätzlich vom Verantwortlichen zu bestimmen; insbesondere ist auch eine elektronische Übermittlung möglich. Nach Möglichkeit sollte die Information in der gleichen Form erteilt werden, in der der Antrag auf Information gestellt wurde; dieser Grundsatz gilt freilich nur, wenn dem keine besonderen Gründe entgegenstehen (vgl. Art. 12 Abs. 1 der Richtlinie (EU) 2016/680). Insbesondere wird etwa im Falle einer telefonischen Antragstellung eine telefonische Auskunft nicht möglich sein, wenn die Identität des Anrufers nicht mit ausreichender Sicherheit festgestellt werden kann. Soweit der Verantwortliche gemäß Abs. 7 zusätzliche Informationen zur Bestätigung der Identität der betroffenen Person anfordert, ist zu beachten, dass diese Informationen nur für diesen konkreten Zweck verarbeitet und nicht länger gespeichert werden dürfen, als es für diesen Zweck notwendig ist (vgl. Erwägungsgrund 41 der Richtlinie (EU) 2016/680).

Der Umgang mit offenkundig unbegründeten oder exzessiven Anträgen gemäß Abs. 6 entspricht der Regelung in Art. 12 Abs. 5 DSGVO. Bei der Beurteilung, ob ein Antrag offenkundig unbegründet oder exzessiv ist, sind die konkreten Umstände im Einzelfall zu berücksichtigen. Darunter kann insbesondere eine rechtsmissbräuchliche Antragstellung fallen, etwa wenn der Antrag vorsätzlich falsche Angaben enthält. Eine wiederholte Antragstellung kann ein Anzeichen für Exzessivität sein, jedoch nicht in Fällen, in denen dies deshalb erfolgt, weil die begehrten Auskünfte zunächst nicht oder nicht vollständig erteilt wurden.

Im Falle einer Verweigerung der Information oder Auskunft oder einer Unterrichtung über die Richtigstellung oder Löschung bzw. Einschränkung der Verarbeitung kann die betroffene Person die Rechtmäßigkeit der Einschränkung ihrer Betroffenenrechte durch die Datenschutzbehörde überprüfen lassen. Die direkte Ausübung der Betroffenenrechte wird dadurch nicht eingeschränkt, sondern vielmehr im Wege des kommissarischen Rechtsschutzes sichergestellt, dass die Rechte der betroffenen Person gewahrt werden und gleichzeitig das mit der Einschränkung verfolgte Ziel nicht vereitelt wird; beispielsweise wird es wohl regelmäßig den Ermittlungserfolg gefährden, wenn sich die Zielperson über die Ausübung der Betroffenenrechte Kenntnis vom Stand der Ermittlungen verschaffen kann.

Die zur Umsetzung des Art. 17 Abs. 1 der Richtlinie (EU) 2016/680 erforderliche Zuständigkeit der Datenschutzbehörde wird durch die Festlegung einer neuen Aufgabe in § 63 Abs. 1 Z 10 geschaffen.

Die Verlängerung der Frist nach § 42 Abs. 4 um weitere zwei Monate kann erfolgen, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Dies wird insbesondere bei der gemeinsamen Verarbeitungen durch mehrere Verantwortliche – und dem dadurch bedingten höheren Aufwand – der Fall sein.

§ 42 Abs. 5 übernimmt inhaltlich Art. 12 Abs. 4 DSGVO. Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er gemäß Art. 12 Abs. 4 DSGVO die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hiefür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. Es erscheint im Sinne der Einheitlichkeit zweckmäßig, für den Bereich der Richtlinie (EU) 2016/680 die gleichen Pflichten wie im Bereich der DSGVO anzuordnen.

Zu § 43:

Mit dieser Bestimmung wird Art. 13 der Richtlinie (EU) 2016/680 umgesetzt. Das Konzept der Informationspflicht nach der Richtlinie (EU) 2016/680 unterscheidet sich grundlegend von der Informationspflicht nach Art. 13 und 14 DSGVO, weil im Strafverfolgungsbereich einerseits besonders detaillierte Regelungen hinsichtlich der Verarbeitung bestehen (und sich viele Informationen somit schon aus dem Gesetz ergeben) und andererseits umfassende Transparenzpflichten, wie sie im Anwendungsbereich der DSGVO geboten sind, den Strafverfolgungszielen zuwiderlaufen können.

Die Informationspflicht ist eine wesentliche Voraussetzung für die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte. Die betroffene Person muss über ein Mindestmaß an Informationen verfügen, die sie in die Lage versetzen, ihre Rechte wahrzunehmen und zB ein Auskunfts- oder Löschungsbegehren an den Verantwortlichen zu richten. Neben dem Umstand, dass personenbezogene Daten verarbeitet werden, müssen betroffenen Personen daher insbesondere grundlegende Informationen wie die Identität des Verantwortlichen, Zweck und Umfang der Verarbeitung sowie der Umfang ihrer Rechte zur Verfügung stehen.

Die Informationspflicht gemäß Abs. 1 bezieht sich auf allgemeine Informationen, die der Verantwortliche allen betroffenen Personen in geeigneter Form zur Verfügung zu stellen hat. Diese Informationen können sich bereits aus der gesetzlichen Grundlage ergeben (insb. Verarbeitungszweck). Neben einer individuellen Information im Einzelfall kommen zur Erfüllung dieser Informationspflicht etwa auch ein Vordruck auf einem Formular (zB Niederschrift einer Einvernahme) oder eine Veröffentlichung, mit der die Informationen der Öffentlichkeit zugänglich gemacht werden (zB Veröffentlichung auf einer Website; vgl. Erwägungsgrund 39 und 42 der Richtlinie (EU) 2016/680), in Frage.

Gemäß Art. 13 Abs. 1 DSGVO teilt der Verantwortliche der betroffenen Person die Informationen gemäß Abs. 1 zum Zeitpunkt der Erhebung dieser personenbezogenen Daten bei der betroffenen Person mit. Für den Fall, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, kommt das Regime des Art. 14 Abs. 3 DSGVO zur Anwendung.

Abs. 2 sieht darüber hinaus eine Information im Einzelfall vor, wenn und soweit dies erforderlich ist, um der betroffenen Person die Ausübung ihrer Rechte zu ermöglichen. Dies ist etwa dann der Fall, wenn die betroffene Person gar keine Kenntnis von der Verarbeitung seiner personenbezogenen Daten hat, weil diese ohne sein Wissen ermittelt wurden (zB im Falle geheimer Ermittlungsmaßnahmen oder bei Erhebung durch Dritte). Dabei ist auf die Umstände im Einzelfall Bedacht zu nehmen. Durch die

individuelle Informationsverpflichtung soll sichergestellt werden, dass die betroffene Person zumindest in die Lage versetzt wird, tätig zu werden und zB ein Auskunftsbegehren an den Verantwortlichen zu richten.

Abs. 3 legt lediglich fest, zu welchem Zeitpunkt die betroffene Person die Informationen gemäß Abs. 1 und 2 erhalten muss, und enthält keine über die Vorgaben des Art. 13 der Richtlinie (EU) 2016/680 hinausgehenden Informationspflichten.

Einschränkungen der Informationspflicht stellen einen Eingriff in das Grundrecht auf Datenschutz der betroffenen Personen (Art. 8 EMRK, Art. 8 GRC, § 1 DSG) dar. Derartige Einschränkungen müssen daher gesetzlich vorgesehen sein, einem der in Abs. 4 genannten Zwecke dienen und in einer demokratischen Gesellschaft erforderlich und verhältnismäßig sein. Die für den Strafverfolgungsbereich vorgesehenen Einschränkungen der Betroffenenrechte im Bereich der Transparenz, der Auskunftsrechte und der Informationspflichten sind aufgrund der besonderen Bedürfnisse im Strafverfolgungskontext erheblich weiter als jene im Anwendungsbereich der DSGVO: Bei den in Abs. 4 Z 1 bis 6 taxativ angeführten Fällen handelt es sich im Regelfall um solche, in denen ein besonders wichtiges öffentliches Interesse – nämlich die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie der Schutz der Rechte und Freiheiten anderer – verfolgt wird und Einschränkungen der Transparenz geboten sein können, um die Tätigkeit der Strafverfolgungsbehörden nicht zu behindern oder gar zu vereiteln.

Gemäß Art. 13 Abs. 4 der Richtlinie (EU) 2016/680 können auf gesetzlicher Ebene Verarbeitungskategorien festgelegt werden, für die einer der in Abs. 4 Z 1 bis 6 genannten Fälle vollständig oder teilweise zur Anwendung kommt. Entsprechende Regelungen wären gegebenenfalls in Materiengesetzen zu treffen.

Zu § 44:

Mit dieser Bestimmung werden die Art. 14 und 15 der Richtlinie (EU) 2016/680 umgesetzt.

Die Dokumentationspflicht (Abs. 4) bezieht sich sowohl auf die rechtlichen als auch auf die sachlichen Gründe für die Nichterteilung der Auskunft.

Nach dem Erwägungsgrund 43 braucht die betroffene Person lediglich im Besitz einer vollständigen Übersicht über diese personenbezogenen Daten in verständlicher Form zu sein, dh. in einer Form, die es ihr ermöglicht, sich dieser Daten bewusst zu werden und nachzuprüfen, ob sie richtig sind und im Einklang mit dieser Richtlinie verarbeitet werden, so dass sie die ihr durch diese Richtlinie verliehenen Rechte ausüben kann. Eine solche Übersicht könnte auch in Form einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, bereitgestellt werden.

Der Auskunftswerber hat am Auskunftsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Verantwortlichen zu vermeiden.

Abs. 5 übernimmt weitgehend die Regelung des § 26 Abs. 8 DSG 2000 und stellt somit klar, dass das Auskunftsrecht wie bisher nicht zur Umgehung von in Materiengesetzen geregelten speziellen Einsichtsrechten (zB Akteneinsicht) verwendet werden kann.

Einschränkungen des Auskunftsrechts sind nur unter den in § 43 Abs. 4 angeführten Voraussetzungen zulässig.

Zu § 45:

Mit dieser Bestimmung wird Art. 16 der Richtlinie (EU) 2016/680 umgesetzt.

Das Recht auf Berichtigung bzw. auf Ergänzung 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 Erwägungsgrund 47 der Richtlinie (EU) 2016/680). Aus diesem Grund kann es erforderlich sein, die Berichtigung oder Vervollständigung mittels einer ergänzenden Erklärung vorzunehmen und somit nachvollziehbar zu machen. Auch das Löschungsrecht unterliegt hier Beschränkungen, da auch Daten, deren Richtigkeit (noch) nicht verifizierbar ist, im Strafverfahren von Bedeutung sein können.

Bei der Löschung ist auch auf die unterschiedlichen Kategorien gemäß § 37 Bedacht zu nehmen.

Einschränkungen der Unterrichtungsverpflichtung sind nur unter den in § 43 Abs. 4 angeführten Voraussetzungen zulässig.

Nach dem Erwägungsgrund 47 sollten personenbezogene Daten mit Einschränkungsmarkierung nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand. Methoden zur Einschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte Daten, beispielsweise zu Archivierungszwecken, auf ein anderes Verarbeitungssystem übertragen oder gesperrt

werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden.

Zu § 46:

Mit dieser Bestimmung werden die Art. 19 und 20 der Richtlinie (EU) 2016/680 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) umgesetzt. Die Verpflichtungen decken sich mit jenen des Art. 24 Abs. 1 und 2 und Art. 25 Abs. 1 und 2 DSGVO, bezieht sich jedoch inhaltlich auf die Einhaltung der Bestimmungen des 3. Hauptstücks.

Die Umsetzung der Maßnahmen gemäß Art. 25 Abs. 1 und 2 darf nicht nur von wirtschaftlichen Erwägungen abhängig gemacht werden. Hat der Verantwortliche eine Datenschutz-Folgenabschätzung vorgenommen, sollten die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt werden (vgl. Erwägungsgrund 53 der Richtlinie (EU) 2016/680). Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern (vgl. Erwägungsgrund 78 der DSGVO).

Zu § 47:

Mit dieser Bestimmung wird Art. 21 der Richtlinie (EU) 2016/680 umgesetzt. Die Vereinbarung nach § 47 muss entsprechend transparent kundgemacht werden. In Fällen mangelnder Transparenz – vor allem hinsichtlich der vorzusehenden Anlaufstelle –, kann die betroffene Person ihre Rechte im Rahmen dieses Hauptstücks bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen. In Fällen, in denen die betreffenden Inhalte und Rollen bereits auf gesetzlicher Ebene vorgegeben sind, kann die Vereinbarung entfallen (zB Zentrales Melderegister).

Zu § 48:

Mit dieser Bestimmung werden die Art. 22 und 23 der Richtlinie (EU) 2016/680 umgesetzt. Diese entsprechen inhaltlich im Wesentlichen den Regelungen in Art. 28 und 29 DSGVO.

Ein Verstoß nach Abs. 7 kann insbesondere dann vorliegen, wenn der Auftragsverarbeiter die Zwecke und Mittel der Verarbeitung entgegen des mit dem Verantwortlichen abgeschlossenen Vertrages selbst bestimmt.

Zu § 49:

Mit dieser Bestimmung wird Art. 24 der Richtlinie (EU) 2016/680 umgesetzt. Aufgrund der inhaltlichen Übereinstimmung mit Art. 30 Abs. 1 bis 4 DSGVO kann – unter Anpassung der darin enthaltenen Verweise – verwiesen werden.

Das Verzeichnis dient dazu, alle Kategorien von Verarbeitungstätigkeiten zu dokumentieren. Die Verzeichnisse sind in schriftlicher bzw. elektronischer Form so zu führen, dass eine nachträgliche Überprüfung der Rechtmäßigkeit der Datenverarbeitung möglich ist.

Zu § 50:

Mit dieser Bestimmung wird Art. 25 der Richtlinie (EU) 2016/680 umgesetzt.

Die Verzeichnisse sind so zu führen, dass eine nachträgliche Überprüfung der Rechtmäßigkeit der Datenverarbeitung möglich ist. Während die Protokollierungspflicht des Art. 25 Abs. 1 der Richtlinie (EU) 2016/680 auf automatisierte Verarbeitungssysteme beschränkt ist, sollen im Rahmen der Umsetzung die nach dem DSG 2000 bestehenden Protokollierungspflichten beibehalten werden; die diesbezüglich bestehenden nationalen Standards können im unionsweiten Vergleich als „best practice“ bezeichnet werden und erzeugen keinen zusätzlichen Aufwand gegenüber der bisherigen Rechtslage, da eine Verpflichtung schon jetzt besteht.

Die Protokollierung in Bezug auf nicht automatisierte Verarbeitungssysteme muss nicht im gleichen Umfang erfolgen wie bei automatisierten Verarbeitungssystemen, da ein automatisches Logging nicht möglich ist. Aus diesem Grund soll für nicht automatisierte Verarbeitungssysteme eine deutlich abgeschwächte – dem § 14 Abs. 2 Z 7 DSG 2000 nachgebildete – Protokollierungspflicht gelten; es muss aber sichergestellt sein, dass der in Abs. 1 festgelegte Zweck der Nachvollziehbarkeit und Überprüfbarkeit der Zulässigkeit der Verarbeitung erreicht wird (vgl. auch Erwägungsgrund 56 der Richtlinie (EU) 2016/680: „Der Verantwortliche oder der Auftragsverarbeiter, der personenbezogene Daten in nicht automatisierten Verarbeitungssystemen verarbeitet, sollte über wirksame Methoden zum

Nachweis der Rechtmäßigkeit der Verarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.“).

Die Verarbeitung von Protokolldaten ist nur in engen Grenzen zulässig. Insbesondere darf die Möglichkeit, diese für Strafverfolgungszwecke zu verwenden, nicht dazu führen, dass diese Maßnahme zum Schutz betroffener Personen zu einer Überwachungsmaßnahme umfunktioniert wird. Eine Verarbeitung ist jedenfalls nur in Bezug auf konkrete Fälle zulässig. Unter „Eigenüberwachung“ sind beispielsweise interne Disziplinarverfahren zu verstehen (vgl. Erwägungsgrund 57 der Richtlinie (EU) 2016/680); auch hiefür ist eine Verarbeitung nur in Bezug auf einen konkreten Fall zulässig. Nicht vom Begriff der Eigenüberwachung umfasst ist hingegen eine Mitarbeiterkontrolle, insbesondere im Sinne einer Leistungs- oder Fehlerkontrolle, soweit diese nicht zur Überprüfung der Rechtmäßigkeit einer Datenverarbeitung erfolgt.

Die in Abs. 2 bezeichneten Verarbeitungsvorgänge umfassen jedenfalls Erhebungen, Veränderungen, Abfragen, Offenlegungen einschließlich Übermittlungen, Kombinationen und Löschungen von personenbezogenen Daten.

Eine gesetzlich festgelegte feste Löschungsfrist für Protokolldaten erscheint nicht zweckmäßig; vielmehr sollten Protokolldaten – wie auch alle anderen personenbezogenen Daten – nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; danach sind die Protokolldaten zu löschen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen. Eine längere Aufbewahrungsdauer muss sich aus besonderen gesetzlichen Vorschriften ergeben.

Zu § 51:

Mit dieser Bestimmung wird Art. 26 der Richtlinie (EU) 2016/680 umgesetzt.

Zu § 52:

Mit dieser Bestimmung wird Art. 27 der Richtlinie (EU) 2016/680 umgesetzt. Die Anforderungen an die Datenschutz-Folgenabschätzung entsprechen den maßgeblichen Anforderungen gemäß Art. 35 DSGVO. Datenschutz-Folgenabschätzungen sollten auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen abstellen, nicht jedoch auf Einzelfälle (vgl. Erwägungsgrund 58 der Richtlinie (EU) 2016/680). Von einem hohen Risiko wird insbesondere in Fällen der Verwendung neuer Technologien auszugehen sein. Sonstige Betroffene können beispielsweise juristische Personen oder bloß wirtschaftlich Betroffene sein.

Zu § 53:

Mit dieser Bestimmung wird Art. 28 der Richtlinie (EU) 2016/680 umgesetzt.

Im Strafverfolgungskontext ist die Verarbeitung personenbezogener Daten im Regelfall vom Gesetzgeber vordeterminiert. Derartige gesetzliche Regelungen begrenzen den Handlungsspielraum sowohl der zuständigen Behörde als auch der Datenschutzbehörde; schriftliche Empfehlungen der Datenschutzbehörde können sich daher nur auf jene Bereiche beziehen, in denen der personenbezogene Daten verarbeitenden zuständigen Behörde entsprechende Möglichkeiten zur Eindämmung des Risikos zur Verfügung stehen. Allfällige Probleme, die sich unmittelbar aus der gesetzlichen Grundlage ergeben und nicht im Wege des Vollzuges gelöst werden können, können nur durch den Gesetzgeber (bzw. allenfalls durch den Verfassungsgerichtshof im Rahmen eines Normenkontrollverfahrens) behoben werden.

Der Konsultationspflicht gemäß Art. 36 Abs. 4 DSGVO wird im Bereich der Bundesgesetzgebung beispielsweise dadurch Genüge getan, dass der Datenschutzbehörde im Rahmen eines Begutachtungsverfahrens Gelegenheit zur Stellungnahme eingeräumt wird. Eine entsprechende Verpflichtung in Bezug auf Gesetzes- und Verordnungsvorhaben auf Länderebene wäre vom Landesgesetzgeber vorzusehen.

Zu § 54:

Mit dieser Bestimmung wird Art. 29 der Richtlinie (EU) 2016/680 umgesetzt. Da die Vorgaben dieser Bestimmung in Bezug auf die Datensicherheit strenger sind als jene des Art. 32 DSGVO, kommt eine Anknüpfung an diese Bestimmung nicht in Betracht.

Zu § 55:

Mit dieser Bestimmung wird Art. 30 der Richtlinie (EU) 2016/680 umgesetzt, wobei in Abs. 1 an die inhaltsgleiche Regelung des Art. 33 DSGVO angeknüpft wird.

Zu § 56:

Mit dieser Bestimmung werden Art. 31 und Art. 12 Abs. 1 und 4 (in Bezug auf Art. 31) Richtlinie (EU) 2016/680 umgesetzt, wobei in Abs. 1 an die inhaltsgleiche Regelung des Art. 34 DSGVO angeknüpft wird.

Zu § 57:

Mit dieser Bestimmung werden die Art. 32 bis 34 der Richtlinie (EU) 2016/680 umgesetzt.

Hinsichtlich der Verpflichtung zur Benennung eines Datenschutzbeauftragten ist eine eigene Regelung erforderlich, weil sich diese nicht vollständig mit der Verpflichtung zur Benennung eines Datenschutzbeauftragten gemäß Art. 37 DSGVO deckt. Im Übrigen soll jedoch die Ausgestaltung des Datenschutzbeauftragten inhaltlich weitgehend an die Vorgaben der DSGVO anknüpfen.

Der Datenschutzbeauftragte soll den Verantwortlichen dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen (vgl. Erwägungsgrund 63 der Richtlinie (EU) 2016/680). Zum Schutz der richterlichen Unabhängigkeit sind davon die Gerichte im Rahmen ihrer justiziellen Tätigkeit ausgenommen.

Unterliegt eine zuständige Behörde in Bezug auf bestimmte Aufgabenbereiche außerhalb der Strafverfolgung der Verpflichtung zur Benennung eines Datenschutzbeauftragten gemäß Art. 38 DSGVO, so kann dieser Datenschutzbeauftragte auch als Datenschutzbeauftragter für den Bereich der Richtlinie (EU) 2016/680 benannt werden.

Zu § 58:

Mit dieser Bestimmung wird Art. 38 der Richtlinie (EU) 2016/680 umgesetzt.

Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen zu den in § 34 genannten Zwecken dürfen nur an für die genannten Zwecke zuständige Behörden im jeweiligen Drittland bzw. in der jeweiligen internationalen Organisation erfolgen. Eine Übermittlung an sonstige Empfänger (zB private Unternehmen) ist hingegen grundsätzlich ausgeschlossen; um allfällige personenbezogene Daten an Private zu übermitteln, sind die in Rechtsschutzabkommen vorgesehenen offiziellen Kanäle einzuhalten.

Auftragsverarbeiter dürfen derartige Übermittlungen nur aufgrund eines ausdrücklichen Auftrages des Verantwortlichen durchführen (vgl. Erwägungsgrund 64 der Richtlinie (EU) 2016/680).

Datenübermittlungen in Drittländer oder internationale Organisationen können aufgrund einer Angemessenheitsentscheidung der Europäischen Kommission, mit der ein angemessenes Datenschutzniveau festgestellt wird (§ 59), falls eine solche nicht vorhanden ist aufgrund geeigneter Garantien (§ 60) oder falls auch diese nicht vorliegen in bestimmten Ausnahmefällen erfolgen (§ 61).

Für die Weiterübermittlung von personenbezogenen Daten, die ursprünglich aus einem anderen Mitgliedstaat stammen, an Drittländer oder internationale Organisationen ist gemäß Abs. 1 Z 3 eine vorherige Genehmigung durch die zuständige Behörde jenes Mitgliedstaats, der die personenbezogenen Daten ursprünglich übermittelt hat, erforderlich. Wird ein derartiges Genehmigungsersuchen von einem anderen Mitgliedstaat der EU gestellt, ist vorbehaltlich abweichender materiengesetzlicher Regelungen zur Erteilung der Genehmigung jene Behörde zuständig, die die personenbezogenen Daten ursprünglich an den anderen Mitgliedstaat übermittelt hat. Von dem Erfordernis einer Vorabgenehmigung kann nur in bestimmten dringenden Ausnahmefällen abgesehen werden.

Um sicherzustellen, dass datenschutzrechtliche Vorgaben nicht dadurch unterlaufen werden können, dass die an ein Drittland oder eine internationale Organisation übermittelten personenbezogenen Daten in der Folge von diesem an ein anderes Drittland oder eine andere internationale Organisation weiterübermittelt werden, muss bei jeder Übermittlung an ein Drittland oder eine internationale Organisation gemäß Abs. 1 Z 5 eine Genehmigungspflicht für derartige Weiterübermittlungen verbindlich verankert werden. Dies kann insbesondere im Rahmen von Polizeikooperations- und Rechtshilfeabkommen erfolgen. Bei der Erteilung dieser Genehmigung sind insbesondere die in Abs. 1 Z 5 angeführten Faktoren zu prüfen und zu berücksichtigen.

Die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, kann die Weiterübermittlung auch an besondere Bedingungen knüpfen (zB Bearbeitungscodes; vgl. Erwägungsgrund 65).

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 6. Mai 2016 geschlossen wurden und die mit dem vor dem genannten Datum geltenden Unionsrecht vereinbar sind,

bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden (siehe Art. 61 der Richtlinie (EU) 2016/680).

Zu § 59:

Mit dieser Bestimmung wird Art. 36 der Richtlinie (EU) 2016/680 umgesetzt, soweit er an die Mitgliedstaaten gerichtet ist.

Die Europäische Kommission kann gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 in Form von Durchführungsakten gemäß Art. 58 Abs. 2 der Richtlinie (EU) 2016/680 beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau bietet. Derartige Angemessenheitsbeschlüsse entsprechen dem Grunde nach den Angemessenheitsbeschlüssen nach Art. 45 DSGVO, sind jedoch inhaltlich auf die Vorgaben der Richtlinie (EU) 2016/680 gerichtet und auf den Strafverfolgungsbereich beschränkt. Eine besondere Genehmigung für Datenübermittlungen aufgrund eines Angemessenheitsbeschlusses ist nicht erforderlich; die Genehmigungspflicht gemäß § 58 Abs. 1 Z 3 bleibt aufrecht.

Angemessenheitsbeschlüsse gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 können von der Europäischen Kommission gemäß Abs. 5 leg.cit. in Form von Durchführungsrechtsakten widerrufen, geändert oder ausgesetzt werden, wenn entsprechende Informationen dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet; Übermittlungen aufgrund angemessener Garantien gemäß § 60 sowie in Ausnahmefällen gemäß § 61 bleiben davon jedoch unberührt.

Die Kommission veröffentlicht gemäß Art. 36 Abs. 8 der Richtlinie (EU) 2016/680 im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländern beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese ein beziehungsweise kein angemessenes Schutzniveau für personenbezogene Daten bieten. Ein zusätzlicher innerstaatlicher Umsetzungsakt ist nicht erforderlich, da § 59 Abs. 1 unmittelbar an das Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 anknüpft.

Vgl. zum Verfahren zur Erlassung von Angemessenheitsentscheidungen Art. 36 Abs. 2 bis 6 der Richtlinie (EU) 2016/680:

„(2) Bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigt die Kommission insbesondere

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und der Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Rechtsinstrumenten sowie aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 dieses Artikels bietet. In dem Durchführungsrechtsakt wird ein Mechanismus für die regelmäßige Überprüfung vorgesehen, die mindestens alle vier Jahre erfolgt und bei der allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich

sowie gegebenenfalls die in Absatz 2 Buchstabe b dieses Artikels genannte Aufsichtsbehörde oder die dort genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 erlassenen Beschlüsse beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen – insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung – dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen gemäß dem in Artikel 58 Absatz 3 genannten Verfahren erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 58 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem Beschluss nach Absatz 5 geführt hat.“

Zu § 60:

Mit dieser Bestimmung wird Art. 37 der Richtlinie (EU) 2016/680 umgesetzt.

Rechtsverbindliche Instrumente iSd Abs. 1 Z 1 können insbesondere Polizei- und Rechtshilfeabkommen sein, die betroffenen Personen subjektive Rechte einräumen und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe vorsehen; bei der Beurteilung der Umstände im Zusammenhang mit der Datenübermittlung gemäß Abs. 1 Z 2 kann der Verantwortliche insbesondere Kooperationsvereinbarungen zwischen Europol oder Eurojust und Drittländern sowie Geheimhaltungspflichten berücksichtigen. Personenbezogene Daten sollten zudem nicht verwendet werden, um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken (vgl. Erwägungsgrund 71).

Zu § 61:

Mit dieser Bestimmung wird Art. 38 der Richtlinie (EU) 2016/680 umgesetzt.

Diese Bestimmung regelt abschließend, unter welchen Voraussetzungen eine Übermittlung personenbezogener Daten zulässig ist, wenn im Drittland bzw. in der internationalen Organisation, an das bzw. an die die Übermittlung erfolgt, kein ausreichendes Datenschutzniveau (dh. weder aufgrund eines Angemessenheitsbeschlusses nach § 59 noch aufgrund geeigneter Garantien gemäß § 60) vorhanden ist. Die in Abs. 1 angeführten Übermittlungszwecke sind taxativ festgelegt; in den Fällen der Z 4 und 5 hat der Verantwortliche zudem eine Interessenabwägung im Einzelfall durchzuführen, in den Fällen der Z 1 bis 3 kann eine solche unterbleiben, weil in diesen Fällen jeweils öffentliche Interessen von besonderem Gewicht betroffen sind, sodass jedenfalls von einem überwiegenden öffentlichen Interesse an der Übermittlung der personenbezogenen Daten auszugehen ist.

Eine Rechtsgrundlage gemäß Abs. 1 Z 2 bilden neben Gesetzen insbesondere auch gesetzesrangige internationale Abkommen sein.

Die Ausnahmen sind restriktiv auszulegen. Häufige, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen in großem Umfang sind auszuschließen und müssen daher auf unbedingt notwendige personenbezogene Daten beschränkt werden (vgl. auch Erwägungsgrund 72).

Um eine Überprüfung der Rechtmäßigkeit derartiger Übermittlung zu ermöglichen, sieht Abs. 3 eine Dokumentationspflicht vor.

Zu § 62:

Nach Art. 41 Abs. 1 der Richtlinie (EU) 2016/680 hat jeder Mitgliedstaat vorzusehen, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Richtlinie zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird. Die Mitgliedstaaten können gemäß Art. 41 Abs. 3 der Richtlinie (EU) 2016/680 auch vorsehen, dass die gemäß der DSGVO in den Mitgliedstaaten errichtete Aufsichtsbehörde die in dieser Richtlinie genannte Aufsichtsbehörde ist und die Verantwortung für die Aufgaben der nach Abs. 1 zu errichtenden Aufsichtsbehörde übernimmt.

In diesem Sinne soll die Datenschutzbehörde sowohl für den Anwendungsbereich der DSGVO als auch der Richtlinie (EU) 2016/680 die zuständige Aufsichtsbehörde nach Art. 41 Abs. 1 und 3 der Richtlinie (EU) 2016/680 sein. Dies wird durch den Verweis auf § 34 sichergestellt. Aufgrund dieses Verweises ist die Datenschutzbehörde aber auch zuständige Aufsichtsbehörde für die Verarbeitung personenbezogener Daten zum Zweck der nationalen Sicherheit, der Nachrichtendienste und der militärischen Eigensicherung.

Nach Art. 45 Abs. 2 der Richtlinie (EU) 2016/680 sieht jeder Mitgliedstaat vor, dass jede Aufsichtsbehörde nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. Die Mitgliedstaaten können vorsehen, dass ihre Aufsichtsbehörde nicht für die Überwachung der von anderen unabhängigen Justizbehörden im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. § 62 Abs. 1 setzt diese Vorgaben des Art. 45 Abs. 2 der Richtlinie (EU) 2016/680 um.

Die Vorgaben für die Unabhängigkeit in Art. 42 der Richtlinie (EU) 2016/680 werden zum einen durch den Verweis auf Art. 52 DSGVO und zum anderen durch den Verweis auf § 8 umgesetzt. Durch den Verweis auf § 8 wird auch zum Teil bereits Art. 44 Abs. 1 lit. f Richtlinie (EU) 2016/680 umgesetzt.

Die allgemeinen Bedingungen für die Mitglieder der Aufsichtsbehörde gemäß Art. 43 sollen durch den Verweis auf Art. 53 DSGVO sowie auf § 7 Abs. 2 sowie auf § 9 umgesetzt werden. Damit sollen überdies auch die Vorgaben des Art. 44 Abs. 1 lit. a bis f Richtlinie (EU) 2016/680 umgesetzt werden.

Zur Umsetzung des Art. 44 Abs. 2 der Richtlinie (EU) 2016/680 ist anzumerken, dass Art. 54 Abs. 2 DSGVO bereits unmittelbar anwendbar die Verschwiegenheitspflicht festlegt. Darüber hinaus gilt für die betroffenen Personen auch die Amtsverschwiegenheit. Insofern kann für die Umsetzung des Art. 44 Abs. 2 der Richtlinie (EU) 2016/680 unmittelbar auf Art. 54 DSGVO verwiesen werden.

Zu § 63:

In jenen Fällen, in welchen der vorliegende Aufgabenbereich in der Richtlinie (EU) 2016/680 grundsätzlich mit jenen der DSGVO ident ist, soll in der Richtlinienumsetzung direkt auf die DSGVO verwiesen werden. Der Verweis auf Art. 57 Abs. 1 lit. c bis e, g, h und t DSGVO ist in Verbindung mit dem Einleitungssatz zu Abs. 1 zu verstehen, welcher auf den Anwendungsbereich des § 34 verweist. Diese Aufgaben sind somit mit der Maßgabe vorzunehmen, dass sie nur den Anwendungsbereich des § 34 in Bezug auf dieses Hauptstück betreffen.

Mit Abs. 3 wird Art. 46 Abs. 3 und 4 der Richtlinie (EU) 2016/680 durch Verweis auf die Bestimmungen in der DSGVO umgesetzt. Die Tätigkeit des Datenschutzbeauftragten ist nach Art. 46 Abs. 3 der Richtlinie (EU) 2016/680 immer unentgeltlich.

Zu § 64:

Ein Verweis auf Art. 58 DSGVO erscheint bei der Umsetzung des Art. 47 der Richtlinie (EU) 2016/680 aufgrund der gänzlich unterschiedlichen Regelungstechnik nicht möglich.

Abs. 2 soll Art. 47 Abs. 2 der Richtlinie (EU) 2016/680 und Abs. 3 soll Art. 47 Abs. 3 der Richtlinie (EU) 2016/680 umsetzen. Abs. 4 sieht die Umsetzung des Art. 47 Abs. 4 der Richtlinie (EU) 2016/680 durch Verweis auf Art. 58 Abs. 4 DSGVO vor.

Abs. 5 soll durch den Verweis auf § 39 Abs. 5 den Art. 47 Abs. 5 der Richtlinie (EU) 2016/680 umsetzen.

Zu § 65:

Die vorgeschlagene Bestimmung zur Umsetzung des Art. 48 der Richtlinie (EU) 2016/680 orientiert sich an bestehenden gesetzlichen Regelungen zum Whistleblowing.

Zu § 66:

Die Datenschutzbehörde hat im Tätigkeitsbericht nach § 12 auch über ihre Tätigkeiten nach dem 3. Hauptstück zu berichten.

Zu § 67:

Für die Umsetzung des Art. 50 der Richtlinie (EU) 2016/680 kann sinngemäß auf die Bestimmungen des Art. 61 Abs. 1 bis 7 DSGVO verwiesen werden, da diese weitgehend inhaltsgleich sind.

Zu § 68:

§ 68 verweist für die Rechtsbehelfe, Haftung und Sanktionen auf den entsprechenden 3. Abschnitt des 2. Hauptstücks. Die Verhängung von Geldbußen gemäß § 19 soll ausgeschlossen sein, da Geldbußen gegen „zuständige Behörden“ (§ 35 Z 7) nicht verhängt werden können.

Zu § 69:

Im Rahmen des Art. 6 Abs. 2 und 3 sowie Art. 23 DSGVO und Kapitel IX der DSGVO iVm Erwägungsgrund 10 können die Mitgliedstaaten spezifischere Vorschriften zum Schutz Privater beibehalten oder erlassen. Derartige Regelungen sollen hinsichtlich der Datenverarbeitungen zu spezifischen Zwecken und der Bildverarbeitungen (5. und 6. Abschnitt des 2. Hauptstücks) vorgesehen werden. Darüber hinaus soll – wie bereits im DSG 2000 – auch das Datengeheimnis (§ 6) in das neue DSG aufgenommen werden. Um bei Verstößen gegen diese Verarbeitungen auch entsprechende Maßnahmen ergreifen zu können, sieht § 69 die Möglichkeit der Verhängung von Verwaltungsstrafen vor.

§ 69 soll nicht zur Anwendung kommen, sofern die Tat einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist; § 69 soll damit nur subsidiär zu diesen Tatbeständen zur Anwendung kommen.

Auch gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach den Vorgaben des § 19 verhängt werden.

Ein Absehen von der Bestrafung für die in § 69 vorgesehenen Strafen ist unter den im VStG vorgesehenen Voraussetzungen möglich (vgl. § 45 Abs. 1 VStG).

Zu § 70:

§ 70 soll den derzeit in § 51 DSG 2000 geregelten gerichtlichen Tatbestand der Datenverarbeitung in Gewinn- oder Schädigungsabsicht weitgehend unverändert in das neue DSG übernehmen.

Zu § 71:

§ 71 enthält den Durchführungs- und Umsetzungshinweis.

Zu § 73:

Verordnungen dürfen unter den in § 73 genannten Voraussetzungen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt. Davon umfasst sind die Verordnungsermächtigungen der Datenschutzbehörde nach § 10 Abs. 2 und 3.

Zu § 76:

Nachdem eine Neueinrichtung der Datenschutzbehörde unionsrechtlich nicht erforderlich ist und die völlige Unabhängigkeit der Datenschutzbehörde beeinträchtigen könnte, sollen die bestehende Leitung sowie ihre Stellvertretung gemäß Abs. 1 bis zum Zeitablauf der seit dem 1. Jänner 2014 laufenden fünfjährigen Funktionsperiode im Amt bleiben. Weiterhin besteht auch die Möglichkeit, dass einzelne Aufgaben oder abgegrenzte Bereiche an entsprechend fachlich geeignete Mitarbeiter delegiert werden.

Abs. 2 regelt das „rechtliche Schicksal“ des Datenverarbeitungsregisters. Dieses soll in bestehender Form zu Archivzwecken für einen Übergangszeitraum bis zum 31. Dezember 2019 weiter erhalten bleiben, wobei jedoch keine Eintragungen oder Änderungen ab dem Inkrafttreten dieses Bundesgesetzes mehr vorgenommen werden dürfen. Eine Archivierung erscheint sinnvoll, um einerseits den Verantwortlichen (Auftraggeber) die Möglichkeit zu geben, etwa für allfällige Dokumentationspflichten oder Datenschutz-Folgenabschätzungen auf diese Ressource zurückzugreifen; andererseits soll auch betroffenen Personen und Behörden – etwa in laufenden Gerichtsverfahren – die Möglichkeit des Zugriffes bis zum 31. Dezember 2019 erhalten bleiben.

Im neuen DSG gibt es keine Möglichkeit für die Erlassung einer Standard- und Musterverordnung; an Stelle dessen hat die Datenschutzbehörde aufgrund von Art. 35 Abs. 4 DSGVO die Möglichkeit, eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, zu erstellen und zu veröffentlichen. Die Datenschutzbehörde kann des Weiteren gemäß Art. 35 Abs. 5 DSGVO eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

Alle auf dem DSG 2000 beruhenden rechtskräftigen Akte der Datenschutzbehörde bleiben aufrecht (vgl. auch die Ausführungen im Erwägungsgrund 171 der DSGVO). Umfasst sind davon insbesondere Genehmigungen der Datenschutzbehörde nach den §§ 13, 46 Abs. 3 und 47 Abs. 3 und 4 DSG 2000. Nicht erfasst sind Registrierungsakte im Datenverarbeitungsregister, dies selbst dann nicht, wenn sie auf § 18 Abs. 2 DSG 2000 (Vorabkontrolle) beruhen. Registrierungen im Datenverarbeitungsregister werden gemäß § 76 Abs. 2 gegenstandslos.

Beruhen die Verarbeitungen auf einer Zustimmung gemäß dem DSG 2000, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Zustimmung den Bedingungen der DSGVO entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der DSGVO fortsetzen kann. Dies entspricht den im

Erwägungsgrund 171 der DSGVO enthaltenen Ausführungen zur „Einwilligung“ nach der Richtlinie 95/46/EG.

Die Abs. 3 bis 6 enthalten Übergangsregelungen für Verfahren.

Gemäß §§ 17 ff DSG 2000 anhängige Registrierungsverfahren sind einzustellen, da die DSGVO und das DSG kein Meldeverfahren mehr kennen.

Ein strafbarer Tatbestand, der vor dem Inkrafttreten dieses Bundesgesetzes verwirklicht wurde, ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren. Dies betrifft nur Anträge an die Datenschutzbehörde. Neue Klagen können bei den ordentlichen Gerichten (§ 5 Abs. 4 DSG 2000) ab dem 25. Mai 2018 daher generell nicht mehr eingebracht werden; stattdessen ist der Antrag an die Datenschutzbehörde zu richten. Der Rechtsmittelzug soll sich für diese ab dem 25. Mai 2018 eingebrachten Fälle ebenfalls nach den Regelungen des neuen DSG richten.

Der Übergang von gerichtlichen Strafverfahren (§ 51 DSG 2000) richtet sich nach den allgemeinen Bestimmungen des Strafrechts.

Abs. 7 regelt die Übergangsbestimmung für den Datenschutzrat. Die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes entsendeten Mitglieder und Ersatzmitglieder des Datenschutzrates sollen bis zum Eintritt einer der Voraussetzungen des § 21 Abs. 5 Z 1 bis 3 in ihrer Funktion bleiben. Mit dieser Bestimmung ist die Kontinuität des Gremiums gesichert. Gleiches gilt sinngemäß auch für den Vorsitzenden des Datenschutzrates und die stellvertretenden Vorsitzenden, die bis zum Eintritt einer der Voraussetzungen des § 22 Abs. 3 Z 1 bis 3 in ihrer Funktion bleiben sollen.

Abs. 8 stellt klar, dass – wie auch schon nach der geltenden Rechtslage – die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (leges speciales) den allgemeinen Regelungen des neuen DSG vorgehen (zB die Verarbeitung personenbezogener Daten im Rahmen der Sicherheitspolizei nach dem 4. Teil des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, oder die organisatorische Einrichtung des Rechtsschutzbeauftragten gemäß § 91a Abs. 1 SPG).

Zu Artikel 3 (Anpassungsbestimmungen)

Zu § 1:

Das DSG 2000 samt den darauf basierenden Verordnungen soll mit Inkrafttreten dieses Bundesgesetzes aufgehoben werden. Auf bestimmte Fälle, die noch einen zeitlichen Bezug zum DSG 2000 haben, kann das DSG 2000 weiterhin beschränkt Anwendung finden (Übergangsregelungen).

In § 1 sollen terminologische und inhaltliche Anpassungen an die DSGVO vorgenommen werden. Diesbezüglich soll der in § 4 Z 4 DSG 2000 definierte Begriff „Auftraggeber“ in allen Bundesgesetzen – wenn in der jeweiligen Bestimmung der „Auftraggeber“ in datenschutzrechtlicher Hinsicht bezeichnet wird – durch den in Art. 4 Z 7 DSGVO definierten Begriff „Verantwortlicher“ in der jeweils grammatikalisch richtigen Form ersetzt werden. Ebenso soll der in § 4 Z 5 DSG 2000 definierte Begriff „Dienstleister“ durch den in Art. 4 Z 8 DSGVO definierten Begriff „Auftragsverarbeiter“ ersetzt werden. Durch die unmittelbare Geltung der DSGVO können die bisher verwendeten Begriffe nicht mehr aufrechterhalten werden.

Hinsichtlich des in Art. 9 DSGVO verwendeten Begriffs der „besonderen Kategorien von personenbezogenen Daten“ wird auf eine Anpassung in Bundesgesetzen verzichtet, zumal der – bislang in der österreichischen Rechtsordnung – verwendete Begriff der „sensiblen Daten“ auch im Erwägungsgrund 10 der DSGVO mit dem Begriff „besondere Kategorien von personenbezogenen Daten“ gleichgesetzt wird.

Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben. Gemäß Art. 94 Abs. 2 DSGVO gelten Verweise auf die aufgehobene Richtlinie als Verweise auf die DSGVO. Eine diesbezügliche Anordnung für das innerstaatliche Recht kann daher unterbleiben.