Entwurf

Erläuterungen

I. Allgemeiner Teil

1. 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 (im Folgenden: DSGVO), tritt am 25.5. 2018 in Geltung.

Der sachliche Anwendungsbereich der DSGVO ist umfassend; die DSGVO gilt gemäß Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die DSGVO nimmt die Tätigkeit der Justiz nicht generell von ihrem sachlichen Anwendungsbereich aus. Vom sachlichen Anwendungsbereich ausgenommen sind lediglich Datenverarbeitungen in den in Art. 2 Abs. 2 DSGVO genannten Bereichen. Gemäß Art. 2 Abs. 2 lit. d gilt die DSGVO nicht für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Die DSGVO gilt daher grundsätzlich für jegliches im Zusammenhang mit einem zivilgerichtlichen Verfahren oder der Tätigkeit in Angelegenheiten der Justizverwaltung ermitteltes personenbezogenes Datum, welches elektronisch (in der Verfahrensautomation Justiz oder in Hinkunft im System der Justiz 3.0) gespeichert wird.

Die DSGVO sieht für den Bereich der justiziellen Tätigkeit lediglich partielle Ausnahmen ihrer Geltung vor. Gemäß Art. 37 Abs. 1 lit. a DSGVO muss kein Datenschutzbeauftragter benannt werden, wenn die Datenverarbeitung von Gerichten vorgenommen wird, die im Rahmen ihrer justiziellen Tätigkeit handeln. Weiters sind gemäß Art. 55 Abs. 3 DSGVO die Aufsichtsbehörden (in Österreich: die Datenschutzbehörde) für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig.

Obwohl die DSGVO unmittelbare Geltung hat und somit grundsätzlich keines weiteren innerstaatlichen Umsetzungsaktes bedürfte, wurde in Durchführung der DSGVO und der Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: DS-RL) das Datenschutz-Anpassungsgesetz 2018 (Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird, BGBl. I Nr. 120/2017) verabschiedet, welches zeitgleich mit der DSGVO in Kraft treten wird.

Die DSGVO enthält auch zahlreiche sogenannte „Öffnungsklauseln“, also fakultative Regelungsspielräume, die den Mitgliedstaaten im sachlichen Anwendungsbereich der Verordnung abweichende oder in bestimmten Bereichen den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten.

In diesem Sinn eröffnet Art. 23 DSGVO die Möglichkeit, durch Rechtsvorschriften der Union oder der Mitgliedstaaten die Pflichten und Rechte gemäß den Art. 12 bis 22 und 34 DSGVO gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Solche Beschränkungen sind überdies nur zur Sicherstellung bestimmter, in den in Art. 23

Abs. 1 lit. a bis j DSGVO angeführter Schutzzwecke zulässig, so etwa zum Schutz der Unabhängigkeit der Justiz und zum Schutz von Gerichtsverfahren (lit. f), zur Sicherstellung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe (lit. g), zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen (lit. i) und zur Sicherstellung der Durchsetzung zivilrechtlicher Ansprüche (lit. j).

Die in den Art. 12 bis 22 und 34 DSGVO angeführten Datenschutzrechte des Einzelnen, die in obigem Sinn gesetzlich eingeschränkt werden können, betreffen etwa das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung.

Die Umsetzung des durch die Öffnungsklauseln eingeräumten gesetzgeberischen Gestaltungsspielraums soll in den spezifischen Materiengesetzen erfolgen.

2. Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Tätigkeit der ordentlichen Gerichtsbarkeit erfordern es, dass von der genannten Öffnungsklausel des Art. 23 DSGVO Gebrauch gemacht wird, um die Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren gewährleisten zu können. Der vorliegende Entwurf sieht daher spezifische Bestimmungen für den Bereich der Justiz und die in enger Verbindung mit der Justiz stehenden Berufsgruppen der Rechtsanwälte und Notare vor.

2.1. Für das zivilgerichtliche Verfahren wird einerseits der Begriff der justiziellen Tätigkeit näher definiert und für das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung, soweit es sich auf den Bereich dieser justiziellen Tätigkeit bezieht, auf die Verfahrensrechte verwiesen. Andererseits wird für die Verletzung des Grundrechts auf Datenschutz ein eigener Feststellungsanspruch, wie er bereits derzeit bei Datenschutzverletzungen durch ein Organ der Gerichtsbarkeit besteht, vorgesehen.

2.2. Darüber hinaus sieht der Entwurf punktuelle Anpassungen im Zivilverfahrensrecht vor, die in der gerichtlichen Praxis derzeit strittige datenschutzrechtliche Fragen auf eine klare gesetzliche Basis stellen sollen.

- Schaffung einer gesetzlichen Grundlage für Gerichte, Akten eines anderen Gerichts unmittelbar im Weg der Verfahrensautomation Justiz und ohne Befassung des anderen Gerichts beizuschaffen.
- Einführung eines Rechtsschutzmechanismus für den Fall, dass ein (inländisches) Gericht einem anderen (inländischen) Gericht die Rechtshilfe durch Übersendung des Gerichtsakts versagt.
- Klärung der Frage, unter welchen Voraussetzungen von Gerichten auf Ersuchen inländischer Verwaltungsbehörden Amtshilfe durch Übersendung von Akten oder Aktenbestandteilen geleistet werden muss.
- Vorgaben für die Veröffentlichung eines Verhandlungsspiegels durch die Gerichte.
- Regelung des Auskunftsrechts von Bürgern über Abfragen des Personenverzeichnisses im Grundbuch durch Notare und Rechtsanwälte.
- Anpassung begrifflicher Änderungen durch die DSGVO.

3. Da der Anwendungsbereich der DSGVO auch das anwaltliche und notarielle Berufsrecht betrifft, werden mit dem Entwurf entsprechende Regelungen in der RAO, NO und DSt vorgeschlagen, die den besonderen Verfahrenszwecken der durch die Rechtsanwälte und Notare geführten Archive, Verzeichnisse und Register (insbesondere Urkundenarchiv, Treuhandregister, ÖZVV und ÖZTR), dem Schutz der berufsrechtlichen Verschwiegenheitspflichten und der Sicherstellung des geordneten Ablaufs von Disziplinarverfahren Rechnung tragen sollen. Die hier vorgesehenen Beschränkungen des Datenschutzrechts und der Begleitrechte nach der DSGVO beziehen sich im Wesentlichen auf die Tatbestände des Art. 23 Abs. 1 lit. g, i und j DSGVO. Auch in diesen Bereichen sollen die besonderen Archiv-, Register- und Verfahrenszwecke dadurch gewahrt werden, dass anstelle der sich aus den Art. 12 bis 22 und 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten die jeweils spezifischen Verfahrensregelungen von RAO, NO, DSt, GOG und der damit im Zusammenhang im selbständigen Wirkungsbereich erlassenen berufsständischen Richtlinien zur Anwendung kommen.

4. Die für den Bereich des Strafrechts geltende Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: DS-RL), ABl. Nr. L 119 vom 4.5.2016 S. 89, wurde durch das Datenschutz-Anpassungsgesetz 2018 und die darin vorgesehenen Anpassungen im Datenschutzgesetz (DSG) idF BGBl. I Nr. 120/2017 umgesetzt.

In dessen 3. Hauptstück finden sich explizite Regelungen zur Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung (§§ 36 ff). Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausdrücklich klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor.

Die bestehenden datenschutzrechtlichen Regelungen der StPO sind daher in erster Linie an die Terminologie der DS-RL (bzw. des DSG) anzugleichen. Ferner soll eine Kriminalpolizei, Staatsanwaltschaft und Gericht gleichermaßen umfassende gesetzliche Grundlage für die grundsätzliche Zulässigkeit der Datenverarbeitung direkt in der StPO verankert und die Akteneinsicht zu wissenschaftlichen Zwecken an die europarechtlichen Vorgaben angepasst werden. Des Weiteren soll der bestehende (subsidiäre) Rechtsschutz des GOG auch weiterhin sowohl im gerichtlichen als auch staatsanwaltschaftlichen Bereich bestehen bleiben.

5. Das der Evidenthaltung strafgerichtlicher Verurteilungen dienende Strafregister unterliegt den unmittelbar anwendbaren Vorschriften der DSGVO. Das StRegG ist daher in erster Linie terminologisch an die Vorgaben der DSGVO anzupassen. Ebenso sind Adaptierungen im Hinblick auf den Rechtsschutz gegen Aufnahmen in das Strafregister und im Zusammenhang mit der Übermittlung von Strafregisterdaten zu wissenschaftlichen Zwecken vorgesehen. Um die dem StRegG (im Einklang mit dem TilgG) wesensimmanenten Schutzzwecke nicht zu unterlaufen, soll ferner klargestellt werden, dass Auskünfte nach der DSGVO ausschließlich in Form einer Strafregisterbescheinigung ergehen sollen.

6. Die DS-RL enthält allerdings auch Regelungen, die den Zuständigkeitsbereich des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz berühren (s. Kapitel V [„Datenübermittlung an Drittländer oder internationale Organisationen“] und Kapitel VI [„Unabhängige Aufsichtsbehörden“]) und einer Umsetzung bedürfen.

II. Besonderer Teil

Zu Artikel 1 (Änderung des Auslieferungs- und Rechtshilfegesetzes):

Zu Ziffer 1 (§ 9a ARHG):

Abs. 1 dieser Bestimmung legt in Umsetzung von Art. 35 bis 38 RL-DS, die Voraussetzungen für die in Erledigung eines Rechtshilfeersuchens erfolgende Übermittlung personenbezogener Daten an einen Drittstaat oder eine internationale Organisation fest, wobei im Hinblick auf den Inhalt von **§ 50** ARHG regelmäßig vom Vorliegen der Voraussetzungen nach **Z 1** auszugehen ist.

Für den Fall, dass die übermittelten Daten aus einem anderen Mitgliedstaat stammen, setzt die Datenübermittlung grundsätzlich das Vorliegen der Zustimmung der zuständigen Behörde des betreffenden Mitgliedstaats voraus (s. **Abs. 1 Z 2**). Die zulässigen Ausnahmen sind in **Abs. 2** angeführt. In einem solchen Fall ist die zuständige Behörde unverzüglich von der Datenweiterleitung in Kenntnis zu setzen.

Es ist davon auszugehen, dass die in **Abs. 1 Z 3, erster Fall** angeführten Voraussetzungen in den seltensten Fällen vorliegen werden, zumal Kommissionsentscheidungen betreffend das Vorliegen eines angemessenen Datenschutzniveaus bisher nur in Bezug auf die Schweiz, Argentinien, Guernsey, die Insel Man, Jersey, die Färöer Inseln, Andorra, Uruguay und Neuseeland ergangen sind.

Abs. 1 Z 3, zweiter Fall betrifft entsprechend Art. 37 Abs. 1 RL DS das Vorliegen angemessener Garantien für den Schutz personenbezogener Daten im betreffenden Staat oder der internationalen Organisation, wobei diese entweder in einem anwendbaren Rechtsinstrument enthalten sein können oder im Einzelfall über entsprechende Nachfrage zugesichert werden (s. lit. a und b *leg. cit*.).

Festzuhalten ist, dass die Angemessenheit der Garantien im Einzelfall entsprechend Art. 37 Abs. 1 lit. b RL DS nach Prüfung aller Umstände, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, vom „Verantwortlichen“ zu beurteilen ist, wobei es sich bei diesem um die aktenführende Behörde (Staatsanwaltschaft oder Gericht) handelt. Zu berücksichtigen wäre dabei u.a., dass die Übermittlung personenbezogener Daten dem Grundsatz der Spezialität unterliegt, damit gewährleistet ist, dass die Daten nicht zu anderen Zwecken als zu jenen, zu denen sie übermittelt wurden, verarbeitet werden. Darüber hinaus sollte berücksichtigt werden, dass die personenbezogenen Daten nicht verwendet werden, um die Todesstrafe oder eine grausame und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken.

Ungeachtet des Vorliegens der Voraussetzungen nach Abs. 1 Z 3 ist die in Erledigung eines Rechtshilfeersuchens erfolgende Datenübermittlung in den in **Abs. 4** genannten Fällen zulässig, wobei wohl regelmäßig von Vorliegen der Voraussetzungen nach **Z 4** auszugehen ist. Festzuhalten ist, dass die Entscheidung im jeweiligen Einzelfall zu treffen ist, wobei zu prüfen ist, ob die Grundrechte des Betroffenen das öffentliche Interesse an der Datenübermittlung überwiegen.

Abs. 5 statuiert entsprechend Art. 38 Abs. 3 RL DS Dokumentationspflichten für den Fall der Datenübermittlung nach Abs. 4. Diese treffen wiederum den Verantwortlichen, somit die aktenführende Behörde. Im Fall der Weiterleitung personenbezogener Daten auf diplomatischem Weg ist die betreffende Verpflichtung für seinen Bereich vom BMEIÄ wahrzunehmen.

Vor dem Hintergrund der elektronischen Aktenführung („ELAK“) und der VJ ist davon auszugehen, dass dadurch den Dokumentationspflichten im Justizbereich ausreichend Rechnung getragen wird.

Zu Ziffer 2 (§ 58a):

Diese Bestimmung enthält in Umsetzung von Art. 35 Abs. 1 lit. e RL DS eine demonstrative Anführung jener Umstände, die von der gemäß **§ 55** zuständigen österreichischen Behörde, die entsprechend **§ 9a Abs. 1 Z 2** um Zustimmung zur Weiterleitung personenbezogener Daten, die in Erledigung eines Rechtshilfeersuchens an einen Drittstaat übermittelt wurden, an einen weiteren Drittstaat oder eine weitere internationale Organisation ersucht wurde, zu berücksichtigen sind.

Zu Ziffer 3 (§ 59a):

Die Datenschutzbestimmung des **§ 9a** idF Z 1 ARHG des Entwurfs gilt vorbehaltlich der Übergangsbestimmung (s. Z 5) für jede Übermittlung personenbezogener Daten durch eine zuständige Behörde, somit auch für die in § 59a ARHG vorgesehene Datenübermittlung ohne Ersuchen. Die in **Abs. 2** dieser Bestimmung enthaltenen Datenschutzbestimmungen hätten daher zu entfallen.

Zu Ziffer 4 (§ 71a):

Art. 39 RL DS sieht unter bestimmten Voraussetzungen die unmittelbare Übermittlung personenbezogener Daten an Empfänger in Drittstaaten vor. Zwar umfasst der Begriff „Empfänger“ nach der RL DS neben natürlichen oder juristischen Personen auch „Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden“, doch soll diese Bestimmung, bei der es sich um eine Kann-Regelung handelt, nur in Bezug auf Personen umgesetzt werden, um eine gesetzliche Grundlage für die unmittelbare Befassung von in Drittstaaten niedergelassenen Providern zu schaffen. Diesbezüglich sind in der Praxis Probleme aufgetreten, da derartige Ersuchen etwa von den zuständigen amerikanischen Behörden keiner Erledigung zugeführt werden; vielmehr wird die ersuchende Behörde aufgefordert, sich unmittelbar mit dem Provider in Verbindung zu setzen, weshalb davon auszugehen ist, dass dieser zur Erteilung entsprechender Informationen an ausländische Behörden ohne weiteres behördliches Dazwischentreten berechtigt ist. Im Hinblick darauf, dass die Befassung des ausländischen Providers wohl regelmäßig durch die entsprechend zu beauftragenden Sicherheitsbehörden erfolgen wird, soll im Einklang mit der österreichischen Rechtslage klargestellt werden, dass eine derartige Vorgangsweise nur in Bezug auf Ersuchen um Übermittlung von Stammdaten, nicht jedoch auch von Verkehrsdaten und Zugangsdaten in Betracht kommt, weil bei Letzteren in der StPO eine qualifizierte Anordnung vorgesehen und sonst eine gerichtliche Bewilligung erforderlich ist (s. **§ 76a Abs. 2 StPO, § 5 Abs. 5 StAG**).

Zu Ziffer 5 (§ 77 Abs. 4):

Diese Bestimmung regelt das Inkrafttreten der §§ 9a, 58a, 59a und 71a und des Art. XXV. Es wird ein Inkrafttreten mit xx.xx.2018 vorgesehen.

Zu Ziffer 6 (Übergangsbestimmung):

Diese Bestimmung stellt in Umsetzung von Art. 61 der RL Datenschutz klar, dass die Datenschutzbestimmung des § 9a auf vor dem 6.5.16 abgeschlossene und mit dem vor diesem Zeitpunkt bestehenden Unionsrecht vereinbare bi- und multilaterale Verträge, die zur Übermittlung personenbezogener Daten führen, keine Anwendung findet. Dies ist eine Folge des Grundsatzes, wonach durch (hier: EU-) Rechtsinstrumente nicht in bestehende Verträge mit Dritten eingegriffen werden kann. Zu denken wäre hier insbesondere an die bestehenden Übereinkommen des Europarats über die justizielle Zusammenarbeit in Strafsachen.

Zu Artikel 2 (Änderung des Bewährungshilfegesetzes):

Zu Z 1 (§§ 3 Abs. 1, 4 Abs. 1 und 3, 5 Abs. 3, 8 Abs. 1, 9, 10, 11, 12 Abs. 1, 13 Abs. 1, 2, 4, 6 und 7, 14, 24 Abs. 1, 3 und 4, 26 Abs. 1 Z 3, 26a Abs. 1, 2 und 3, 28 Abs. 1, 2 und 3, 29 Abs. 1, 29d Abs. 1 lit. b und 31 BewHG):

Mit den vorgeschlagenen Änderungen soll die Erweiterung des Bundesministeriums für Justiz zum Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz durch die Bundesministeriengesetz-Novelle 2017, BGBl. I Nr 164/2017, nachvollzogen werden.

Zu Z 2 (§ 25 BewHG):

Die vorgeschlagenen Änderungen dienen der Anpassung an das DSG („Verarbeitung“ statt „Verwendung“, „personenbezogene Daten“ statt „sensible Daten“ sowie § 38 DSG idF BGBl. I Nr. 120/2017 entsprechende Kautelen).

Zu Artikel 3 (Änderung des Disziplinarstatuts für Rechtsanwälte und Rechtsanwaltsanwärter):

Zu Z 1 (§ 20 DSt):

Zum vorgeschlagenen § 20 Abs. 4 und 5 DSt darf zunächst auf die Ausführungen zum vorgeschlagenen § 84 GOG verwiesen werden. Eine der dort näher beschriebenen „Öffnungsklauseln“ der DSGVO, die den Mitgliedstaaten als fakultative Regelungsspielräume im Anwendungsbereich der Verordnung unter bestimmten Voraussetzungen abweichende oder auch den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten, betrifft (auch) den Bereich des anwaltlichen (wie auch des notariellen) Disziplinarrechts.

Konkret sind nach Art. 23 Abs. 1 lit. g DSGVO Beschränkungen der in den Art. 12 bis 22 und Art. 34 sowie Art. 5 DSGVO vorgesehenen Rechte und Pflichten im Weg von Gesetzgebungsmaßnahmen dann zulässig, wenn die Beschränkung der Sicherstellung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe dient. Erforderlich ist ferner, dass die Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt.

Von dieser Öffnungsklausel soll im Bereich des Verfahrens vor dem Disziplinarrat der Rechtsanwaltskammer und dem Kammeranwalt dahingehend Gebrauch gemacht werden, dass sich die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung nach dem 5. Abschnitt des DSt richten.

Dahinter steht die Überlegung, dass das anwaltliche Disziplinarverfahren auch in erster Instanz besonderen verfahrensrechtlichen Anforderungen gerecht werden muss, um einerseits den – dem übergeordneten Interesse einer geordneten Rechtspflege dienenden – Anspruch auf wirksame Verfolgung von Verstößen gegen das anwaltliche Berufs- und Standesrecht hinreichend zu gewährleisten und andererseits den Vorgaben des Rechts auf ein faires Verfahren gemäß Art. 6 EMRK zu entsprechen.

Unter Beachtung dieser Zielsetzungen enthält das DSt in seinem 5. Abschnitt ein ausgewogenes Regulativ dazu, wie die Ermittlung der für die Beurteilung der an den Kammeranwalt bzw. den Disziplinarrat herangetragenen disziplinarrechtlichen Vorwürfe gegen einen Rechtsanwalt (oder Rechtsanwaltsanwärter) benötigten Daten zu erfolgen hat und wie diese verwendet werden dürfen (vgl. §§ 22 und 27 ff. DSt). Ebenso geregelt sind die Informations- und Auskunftsrechte des Beschuldigten (siehe ua. § 22 Abs. 4 und § 27 Abs. 2 DSt) und die Frage (des Umfangs des Rechts) der Akteneinsicht (§ 27 Abs. 5 und § 31 Abs. 5 DSt).

Das verfahrensrechtliche Regime des 5. Abschnitts des DSt entspricht von seinem Wesen und seinem Inhalt her insgesamt den Anforderungen an ein formelles gerichtliches Verfahren; dies wird nicht zuletzt durch die in § 77 DSt ergänzend angeordnete sinngemäß Anwendung von Bestimmungen der StPO deutlich. Dieses Verfahrensrecht regelt dabei die Informations- und Auskunftsrechte, die Frage der Ermittlung und Verarbeitung der Daten und deren Verwendung auf eine Weise, die – unter Berücksichtigung datenschutzrechtlicher Vorgaben – die effektive Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen das Berufs- und Standesrecht der Rechtsanwälte sicherstellt. Es erscheint daher in Anwendung der Öffnungsklausel des Art. 23 Abs. 1 lit. g DSGVO legitim und gerechtfertigt, die (im Sinn der DSGVO) von einem anwaltlichen Disziplinarverfahren betroffene Person zur Durchsetzung ihres Rechts auf Schutz bei der Verarbeitung personenbezogener Daten im Verfahren vor dem Disziplinarrat und dem Kammeranwalt insgesamt auf dieses besondere Regulativ zu verweisen.

Die Umstände können es dabei gerade im Verhältnis zum Beschuldigten auch erfordern, Informationen oder Auskünfte zum Disziplinarverfahren soweit und solange aufzuschieben, einzuschränken oder zu unterlassen, wie dies im Einzelfall zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von Disziplinarvergehen unbedingt erforderlich und verhältnismäßig ist. Zu denken ist dabei etwa an

Konstellationen, wo aufgrund entsprechender (frühzeitiger) Bekanntgaben Verdunkelungsgefahr besteht oder die Sicherstellung von Beweismitteln vereitelt werden könnte. Mit dem – § 43 Abs. 4 DSG idF BG BGBl. I Nr. 120/2017 entsprechenden – vorgeschlagenen § 20 Abs. 5 DSt soll diesem Erfordernis Rechnung getragen werden.

Zur Entscheidung über Rechtsmittel gegen Erkenntnisse des Disziplinarrats ist gemäß § 46 DSt der Oberste Gerichtshof zuständig. Da es sich insofern um ein ordentliches gerichtliches Verfahren handelt, erübrigen sich im vorliegenden Kontext gesonderte datenschutzrechtliche Anordungen dazu im DSt.

Zu Artikel 4 (Änderung der EO):

Zu Z 1 und 2 (§ 275 Abs. 6 und § 382g Abs. 1 EO):

In § 275 Abs. 6 und § 382g Abs. 1 Z 4 werden terminologische Anpassungen aus Anlass der Datenschutz-Grundverordnung vorgenommen.

Zu Artikel 5 (Änderung des GOG):

Zu Z 1 (§ 16a GOG):

Mit der vorgeschlagenen Bestimmung soll eine ausdrückliche gesetzliche Grundlage für die Veröffentlichung eines sogenannten „Verhandlungsspiegels“ durch die Gerichte geschaffen werden.

Durch die Veröffentlichung eines Verhandlungsspiegels soll es der Bevölkerung erleichtert werden, sich einen Überblick über den Ort, den Tag, die Stunde des Beginns und den Gegenstand des Verfahrens der am jeweiligen Gericht stattfindenden öffentlichen Gerichtsverhandlungen in bürgerlichen Rechtssachen und in Strafsachen zu verschaffen. Mit der vorgeschlagenen Regelung soll klargestellt werden, dass die Allgemeinheit nur über öffentliche Gerichtsverhandlungen entsprechend informiert werden soll und dass im Verhandlungsspiegel in bürgerlichen Rechtssachen auch die Namen der Parteien ersichtlich sein dürfen, weil der verfassungsrechtlich verankerte Schutz des Grundsatzes der Öffentlichkeit von Gerichtsverhandlungen (Ar. 6 EMRK) insoweit das Geheimhaltungsinteresse überwiegt.

Ob solche Verhandlungsspiegel überhaupt erstellt und in welcher Form sie von den Gerichten veröffentlicht werden (etwa durch Aushang am „schwarzen Brett“, Darstellung auf einem Infoscreen oder auf der Website des Gerichts), bleibt der Entscheidung der zuständigen Organe der Justizverwaltung überlassen.

Zu Z 2 (§§ 83 bis 85a GOG):

Datenverarbeitungen in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der weisungsfreien Justizverwaltung fallen in den Anwendungsbereich der DSGVO, die am 25.5.2018 in Geltung tritt.

Datenverarbeitungen in Angelegenheiten der Strafgerichtsbarkeit fallen in den Anwendungsbereich der Richtlinie (EU) 2016/680 (im Folgenden: DS-RL), die mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, umgesetzt wurde, welches gemeinsam mit der DSGVO in Kraft treten wird.

Demnach ist es erforderlich, die bestehenden datenschutzrechtlichen Regelungen der §§ 83 bis 85 GOG an die (teilweise) neuen rechtlichen Gegebenheiten und Instrumentarien der DSGVO und des DSG für den Bereich der Datenverarbeitungen in Angelegenheiten der Gerichtsbarkeit anzupassen.

Da nun nicht mehr – wie bisher mit dem DSG 2000 – ein einheitliches datenschutzrechtliches Regelungswerk besteht, ist es erforderlich, in Anpassung an die rechtlichen Vorgaben der DSGVO und des neuen Datenschutzgesetzes getrennte Regelungen für die Gerichtsbarkeit in bürgerlichen Rechtssachen und der weisungsfreien Justizverwaltung einerseits (§§ 83 bis 85 des Entwurfs) sowie für Angelegenheiten der Strafgerichtsbarkeit andererseits (§ 85a des Entwurfs) vorzusehen.

Zu § 83 GOG:

Im vorgeschlagenen § 83 Abs. 1 ist statuiert, dass die Gerichte im Rahmen ihrer justiziellen Tätigkeit die hiefür erforderlichen personenbezogenen Daten verarbeiten dürfen.

Diese generelle Festlegung trägt dem sowohl im innerstaatlichen wie auch im europäischen Datenschutzrecht geltenden Prinzip Rechnung, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, wenn der Gesetzgeber nicht ausdrücklich eine Erlaubnis erteilt. Die näheren Umstände, welche Daten für welche Zwecke und in welchem Umfang von den Gerichten ermittelt und auf welche Weise diese verarbeitet werden dürfen sowie alle weiteren für die gerichtlichen Datenverarbeitungen geltenden Grundsätze werden durch die von den Gerichten einzuhaltenden Verfahrensgesetze und den darauf beruhenden Verordnungen sowie den Vorschriften des GOG determiniert. Dabei wird in Hinkunft auch Art. 5 DSGVO als Leitlinie für die (europarechtskonforme) Auslegung der nationalen Bestimmungen dienen.

Der bereits im vorgeschlagenen § 83 Abs. 1 verwendete Begriff der „justiziellen Tätigkeit“ der Gerichte soll im vorgeschlagenen § 83 Abs. 2 definiert werden. Dieser Begriff wird in der DSGVO im Zusammenhang mit den Bereichsausnahmen der Artikel 37 Abs. 1 lit. a (Benennung eines Datenschutzbeauftragten) und Artikel 55 Abs. 3 (Aufsichtsbehörden) verwendet. In Erwägungsgrund 20 der DSGVO wird damit im Zusammenhang ausgeführt, dass die Aufsichtsbehörden (in Österreich: die Datenschutzbehörde) nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein sollen, damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassungen unangetastet bleibt.

Im Sinne dieses Begriffsverständnisses, welches ausdrücklich den Schutz der Unabhängigkeit der Justiz und den Begriff der justiziellen Tätigkeit der Gerichte in einen Bedeutungszusammenhang stellt, wird im vorgeschlagenen § 83 Abs. 2 festgelegt, dass die justizielle Tätigkeit der Gerichte alle Tätigkeiten umfasst, die zur Erfüllung der Aufgaben in Angelegenheiten der ordentlichen Gerichtsbarkeit erforderlich sind.

Durch die Formulierung „in Angelegenheiten der ordentlichen Gerichtsbarkeit“ soll deutlich gemacht werden, dass der Anwendungsbereich des vorgeschlagenen § 83 – ebenso wie dies beim geltenden § 83 GOG der Fall ist – nicht nur die gerichtliche Entscheidungstätigkeit als Kernbereich der unabhängigen Rechtsprechung umfassen soll, sondern auch die in Senaten ausgeübte Justizverwaltung, die ebenfalls als Gerichtsbarkeit im formellen Sinn zu betrachten ist. Sofern Aufgaben der Justizverwaltung kollegial zu besorgen sind, werden die Richter in Ausübung ihres richterlichen Amtes tätig und liegt eine Vollziehung durch Gerichtsbehörden vor (vgl. Art. 87 Abs. 2 B-VG; VfSlg. 7753/1976, 13.215/1992, 19.618/2012).

Ebenso Teil der justiziellen Tätigkeit der Gerichte sind die Aufgaben und Befugnisse, die im Zusammenhang mit dem Verlassenschaftsverfahren den Notaren in ihrer Funktion als Gerichtskommissäre gesetzlich zugewiesen sind. Auch die Befundaufnahme und Gutachtenserstattung der gerichtlich bestellten Sachverständigen ist Teil des gerichtlichen Beweisverfahrens und gehört somit in diesem Umfang zur justiziellen Tätigkeit der Gerichte.

Soweit die Tätigkeit der Justizverwaltung nicht in Senaten vollzogen wird, ist diese nicht als justizielle Tätigkeit der Gerichte im Sinn der DSGVO und des vorgeschlagenen § 83 Abs. 2 GOG zu qualifizieren.

Zu § 84 GOG:

Die DSGVO und das DSG nehmen die Tätigkeit der Justiz nicht generell von ihrem sachlichen Anwendungsbereich aus. Die datenschutzrechtlichen Vorgaben der DSGVO und des DSG gelten demnach grundsätzlich für jegliches im Zusammenhang mit einem zivilgerichtlichen Verfahren oder der Tätigkeit in Angelegenheiten der Justizverwaltung ermitteltes personenbezogenes Datum, welches elektronisch (in der Verfahrensautomation Justiz oder in Hinkunft im System Justiz 3.0) gespeichert wird. Die DSGVO enthält jedoch sogenannte „Öffnungsklauseln“, also fakultative Regelungsspielräume, die den Mitgliedstaaten im sachlichen Anwendungsbereich der Verordnung abweichende oder in bestimmten Bereichen den Schutzbereich der DSGVO einschränkende nationale Regelungen gestatten.

In diesem Sinn legt Art. 23 DSGVO nähere Voraussetzungen für allfällige Beschränkungen der Betroffenenrechte gemäß den Art. 12 bis 22 und 34 DSGVO in konkreten Konstellationen sowie Vorgaben in Bezug auf die gesetzliche Ausgestaltung fest. Sieht das nationale Recht derartige Beschränkungen vor, so müssen diese Regelungen den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Solche Beschränkungen sind überdies nur zur Sicherstellung bestimmter, in den in Art. 23 Abs. 1 lit. a bis j DSGVO angeführter Schutzzwecke zulässig, so etwa zum Schutz der Unabhängigkeit der Justiz und zum Schutz von Gerichtsverfahren (lit. f).

Die in den Art. 12 bis 22 und 34 DSGVO angeführten Datenschutzrechte des Einzelnen, die in obigem Sinn gesetzlich eingeschränkt werden können, betreffen etwa das Recht auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung. In ähnlicher Weise ermöglicht § 1 Abs. 4 DSG bei Eingriffen staatlicher Behörden zur Wahrung überwiegender berechtigter Interessen eines anderen gesetzliche Beschränkungen der Rechte auf Auskunft, Richtigstellung und Löschung gemäß § 1 Abs. 3 DSG, wenn diese den Voraussetzungen des § 1 Abs. 2 DSG genügen, also insbesondere aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und der Eingriff verhältnismäßig ist.

Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Tätigkeit der ordentlichen Gerichtsbarkeit erfordern es, dass von der genannten Öffnungsklausel des Art. 23 DSGVO bzw. § 1 Abs. 4 DSG Gebrauch gemacht wird, um die Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren zu gewährleisten. Der dabei im vorgeschlagenen § 84 verfolgte Grundgedanke lautet, dass sich bei Datenverarbeitungen im

Rahmen der justiziellen Tätigkeit in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der in Senaten zu erledigenden Justizverwaltung die sich aus Art. 12 bis 22 und Art. 34 DSGVO und die sich aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung nach den Verfahrensgesetzen und den darauf beruhenden Verordnungen sowie den Vorschriften des GOG richten. Diese Abgrenzung entspricht auch der derzeitigen Rechtslage und Judikatur zum Datenschutz in Angelegenheiten der Gerichtsbarkeit gemäß §§ 83 bis 85 GOG in der derzeit geltenden Fassung.

Die im Gerichtsverfahren (insbesondere im Beweisverfahren) notwendige Verwendung von Daten muss speziellen Zielsetzungen gerecht werden. Die Gerichtsbarkeit in bürgerlichen Rechtssachen muss den Rechtsverfolgungsanspruch und gleichzeitig den Rechtsverteidigungsanspruch der Parteien unter Beachtung der Vorgaben des Rechts auf ein faires Verfahren gemäß Art. 6 EMRK wahren. Dritte Personen dürfen nur ausnahmsweise und in speziell geregelten Konstellationen Einblick in die Verfahrensinhalte bekommen. Rechtsfürsorgeverfahren, wie etwa im Bereich der Erwachsenenschutz- oder Kindschaftsverfahren, verfolgen hingegen andere Verfahrenszwecke und stellen die Interessen der schutzberechtigten Personen in den Vordergrund. Es erfordert daher ein ausdifferenziertes und auf die Bedürfnisse der jeweiligen Verfahrensart abgestelltes Regulativ, welche Daten vom Gericht ermittelt und wie diese verwendet werden dürfen. Die entsprechenden gesetzlichen Grundlagen finden sich in den maßgebenden Verfahrensgesetzen (insbesondere ZPO, AußStrG und JN), in den darauf beruhenden Verordnungen (insbesondere die Geo.) sowie im GOG. Diese Bestimmungen nehmen, sofern sie die Rechte und Pflichten gemäß den Art. 12 bis 22 und 34 DSGVO sowie § 1 Abs. 3 DSG (teilweise) beschränken, die von Art. 23 Abs. 2 DSGVO und § 1 Abs. 2 DSG geforderten Wertungen und Abwägungen vor.

Die gerichtlichen Verfahrensgesetze, die darauf basierenden Verordnungen und das GOG regeln die datenschutzrechtlichen Rechte und Pflichten für den Bereich der Gerichtsverfahren abschließend.

Derselbe Grundsatz gilt für die Angelegenheiten der in Senaten zu erledigenden Justizverwaltung. Auch bei diesen Agenden der unabhängigen richterlichen Tätigkeit müssen spezifische Verfahrenszwecke gewahrt werden, weshalb ein abweichendes datenschutzrechtliches Regulativ auch in diesem Bereich erforderlich ist. Zu diesen Angelegenheiten zählen etwa die Geschäftsverteilung für die gerichtlichen Geschäfte, die Besetzungsvorschläge für die ausgeschriebenen Richterplanstellen und die Dienstbeschreibungen der Richter (vgl. *Fellner/Nogratnig*, RStDG – GOG[4] [2015] § 31 GOG Anm 6).

Die Verfahrensgesetze gestalten somit die Rechte auf Auskunft und Information, auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung auf eine Art und Weise, die – unter Berücksichtigung datenschutzrechtlicher Vorgaben – das Funktionieren und die Unabhängigkeit der Gerichtsbarkeit sicherstellen. In manchen Bereichen gehen die durch die Verfahrensgesetze eingeräumten Rechte über die von der DSGVO eingeräumten hinaus, in manchen Bereichen sind sie nur umgestaltet und in anderen Bereichen wiederum eingeschränkt oder ausgeschlossen.

So sind beispielsweise Parteien und Zeugen grundsätzlich verpflichtet, im gerichtlichen Verfahren Auskunft über personenbezogene Daten zu erteilen. Zur Gewährleistung bestimmter überwiegender persönlicher Interessen an der Geheimhaltung bestimmter Informationen enthalten die Verfahrensgesetze detaillierte Regelungen, unter welchen Voraussetzungen bzw. in welchem Umfang Parteien oder Zeugen – zur Wahrung auch ihres datenschutzrechtlichen Widerspruchsrechts – die Beantwortung von Fragen verweigern dürfen (so die §§ 321 ff, § 380 ZPO, die gemäß § 35 AußStrG auch im außerstreitigen Verfahren anzuwenden sind).

Für die Frage, unter welchen Umständen der Gegenpartei oder einem Dritten die Vorlage von Urkunden aufgetragen werden kann, enthalten die (gemäß § 35 AußStrG auch im außerstreitigen Verfahren anwendbaren) §§ 298 ff ZPO detaillierte Regelungen, deren Einhaltung die entsprechenden Anordnungen des Gerichtes auch datenschutzrechtlich absichert.

Anstelle des datenschutzrechtlichen Auskunfts- und Informationsrechts steht den Parteien das Recht auf Akteneinsicht zu. Das über das Recht auf Akteneinsicht Erlangbare geht weit über den Umfang jener Information hinaus, die im Wege der datenschutzrechtlichen Auskunfts- und Informationserteilung zu erzielen ist. Da die Gerichte in erster Linie personenbezogene Daten der Verfahrensparteien verarbeiten, werden die datenschutzrechtlichen Vorgaben für den Großteil der von der Gerichtsbarkeit verarbeiteten Daten in diesem Bereich übererfüllt. Die grundsätzlich in jeder Phase des Gerichtsverfahrens zu wahrende Parteiöffentlichkeit gewährleistet somit das datenschutzrechtliche Informations- und Auskunftsrecht.

Lediglich das Recht dritter Personen, deren Daten Eingang in Gerichtsverfahren finden, wie Zeugen, Dolmetscher oder Sachverständiger, auf Auskunft und Information ist nur eingeschränkt gegeben. Ihnen stehen Akteneinsichtsrechte nur soweit zu, als sie auch Parteistellung haben (zB bei Verhängung von

Ordnungsstrafen gegen Zeugen, Gebührenbestimmung des Sachverständigen) oder ein rechtliches Interesse dartun können. Die verarbeiteten Daten der Parteien sollen nicht oder nur im unbedingt nötigen Ausmaß für andere Personen zugänglich sein. § 219 ZPO sieht daher nur für die Parteien des Verfahrens ein uneingeschränktes Recht auf Akteneinsicht vor. Fehlt eine Zustimmung der Parteien, so können Dritte nur insoweit Akteneinsicht erlangen, als sie ein rechtliches Interesse glaubhaft machen. Es ist im Einzelfall zu prüfen, ob die Akteneinsicht unbedingt nötig ist oder ob sie einen unverhältnismäßigen Eingriff in Geheimhaltungsrechte anderer im Akt aufscheinender Personen darstellt, wobei bei dieser Abwägung auch die Geheimhaltungsinteressen im Akt aufscheinender (anderer) Dritter zu berücksichtigen sind.

Soweit in besonderen Konstellationen Auskunftsrechte zur Wahrung von Geheimhaltungsinteressen bzw. zur Geltendmachung von Verletzungen des Grundrechts auf Datenschutz erforderlich sind, sollen diese durch Sonderregeln geschaffen werden. So sieht etwa § 6a Grundbuchsumstellungsgesetz einen eigenen Auskunftsanspruch über Abfragen aus dem Personenverzeichnis des Grundbuchs vor, ebenso § 430 EO über Abfragen aus bestimmten Daten aus einem Exekutionsverfahren (tritt mit 1. Jänner 2019 in Kraft).

Das Recht auf Richtigstellung und Löschung ist eng an den Zweck der Datensammlung gebunden: für die Beurteilung, ob ein in einem Register, Geschäftsbehelf oder Gerichtsakt enthaltenes Datum „richtig“ oder „unrichtig“, „zulässig“ oder „unzulässig“ ist, ist nämlich nicht auf seine „objektive“ Richtigkeit, sondern auf den Zweck und die vorhersehbare Verwendung der Datensammlung abzustellen. Ein Recht auf Richtigstellung von personenbezogenen Daten besteht im Zusammenhang mit gerichtlichen Verfahren daher nur ausnahmsweise (etwa im Antrag auf Richtigstellung der Parteibezeichnung, auf Berichtigung einer Entscheidung oder den Vorschriften zur Richtigstellung des gerichtlichen Protokolls). Gerade im Beweisverfahren ermittelte Daten müssen in der Weise, wie diese in das Verfahren Eingang gefunden haben, auch zum Akteninhalt gemacht werden. Auch falsche Angaben zu Personen können für das Gerichtsverfahren von Relevanz sein und dürfen daher nicht nachträglich einer „Korrektur“ zugänglich sein.

Die Regeln der §§ 173 ff. Geo. zur Aktenvernichtung legen fest, welche Akteninhalte zu welchem Zeitpunkt zu löschen sind, und gewährleisten dadurch das datenschutzrechtliche Recht auf Löschung.

Was die öffentlichen Bücher (Register), insbesondere Grund- und Firmenbuch, betrifft, so sind die durch die vorgeschlagene Bestimmung getroffenen Abweichungen von den Rechten und Pflichten der Art. 12 bis 22 und 34 DSGVO zum Schutz der betreffenden Gerichtsverfahren und der Unabhängigkeit der Justiz wie folgt zu begründen:

Das Grundbuch ist ein von den Bezirksgerichten in ihrer justiziellen Tätigkeit geführtes öffentliches Verzeichnis, in das Grundstücke und die an ihnen bestehenden dinglichen Rechte eingetragen werden. Es dient der Sicherung des Rechtsverkehrs durch Offenkundigkeit der Rechtsverhältnisse. Dingliche Rechte an Liegenschaften können – von einigen Ausnahmen abgesehen – nur durch Eintragung in das Grundbuch erworben werden. Das Vertrauen des gutgläubigen rechtsgeschäftlichen Erwerbers auf die Richtigkeit und Vollständigkeit des Grundbuchs ist geschützt.

Daraus folgt zum einen, dass die in das Grundbuch eingetragenen personenbezogenen Daten jedermann zur Einsicht offenstehen müssen. Das Grundbuchsumstellungsgesetz sieht eine Einschränkung dieses Grundsatzes nur insofern vor, als es für die Einsicht in das Personenverzeichnis ein rechtliches Interesse verlangt.

Darüber hinaus müssen aus der Einsicht in das Grundbuch auch die Kette der Rechtserwerbe und Rechtsverluste lückenlos nachvollziehbar sein. Nicht mehr aktuelle oder zu berichtigende ursprünglich unrichtige Grundbuchseintragungen werden aus diesem Grund nur im Hauptbuch gelöscht und in das Verzeichnis der gelöschten Eintragungen (§ 3 GUG) aufgenommen, das dem Hauptbuch gleichsteht und wie dieses von jedermann einsehbar ist.

Das – aus dem Hauptbuch und der Urkundensammlung bestehende – Firmenbuch wird von den Gerichten in ihrer justiziellen Tätigkeit geführt (vgl. § 7 UGB) und dient der Offenlegung von Tatsachen, die nach dem Firmenbuchgesetz (FBG) oder nach sonstigen gesetzlichen Vorschriften einzutragen sind (vgl. § 1 Abs. 2 FBG). Es ist also gesetzlich genau festgelegt, welche Rechtsträger in das Firmenbuch einzutragen sind, welche Angaben die Eintragungen zu enthalten haben und welche Urkunden in die Urkundensammlung aufzunehmen sind. Für Kapitalgesellschaften ist die Offenlegung von bestimmten Urkunden und Angaben in einem öffentlichen Register auch unionsrechtlich geboten (vgl. Art. 14 ff. der Richtlinie 2017/1132 über bestimmte Aspekte des Gesellschaftsrechts).

Eintragungen in das Firmenbuch erfolgen in aller Regel auf Antrag. Dabei kann die Identität des Antragstellers verlässlich geprüft werden, weil die Unterschrift des Antragstellers grundsätzlich der gerichtlichen oder notariellen Beglaubigung bedarf (vgl. § 11 Abs. 1 UGB). Teilweise bestehen auch für

die der Anmeldung zugrundeliegenden Rechtsgeschäfte (z.B. den Abschluss eines Gesellschaftsvertrags) besondere Formpflichten (z.B. Notariatsaktsform), was eine verlässliche Dokumentation der Vorgänge und eine Vorabprüfung ihrer Rechtmäßigkeit gewährleistet.

Das Firmenbuchgericht ist zu einer genauen Prüfung der Anmeldung und ihrer Beilagen verpflichtet und darf eine Eintragung im Firmenbuch nur vornehmen, wenn alle formellen und materiellen Voraussetzungen erfüllt sind. Die maßgeblichen Verfahrensvorschriften finden sich im FBG, das in seinem § 15 Abs. 1 auch eine subsidiäre Geltung des AußStrG anordnet. Demnach liegt jeder Eintragung ein entsprechender Beschluss des Firmenbuchgerichts zugrunde, gegen den gegebenenfalls ein Rechtsmittel (Rekurs) erhoben werden kann. Von vornherein unzulässige oder unzulässig gewordene Eintragungen kann das Gericht auch von Amts wegen löschen (vgl. § 10 Abs. 2 FBG).

Ändert sich eine im Firmenbuch eingetragene Tatsache, so ist der Rechtsträger zur unverzüglichen Anmeldung dieser Änderung verpflichtet (vgl. § 10 Abs. 1 FBG). Diese Verpflichtung kann – wie alle Verpflichtungen zur Vornahme einer Anmeldung oder Einreichung zum Firmenbuch – mit einer vom Firmenbuchgericht zu verhängenden Zwangsstrafe durchgesetzt werden. Dadurch wird gewährleistet, dass gesetzlich vorgeschriebene Anmeldungen auch tatsächlich vorgenommen werden.

Zu § 85 GOG:

Der vorgeschlagene § 85 GOG entspricht im Wesentlichen der geltenden Bestimmung.

Mit der vorgeschlagenen Fassung wird die Bestimmung im Hinblick auf § 85a GOG des Entwurfs, welcher nunmehr den Rechtsschutz bei Verletzungen im Grundrecht auf Datenschutz in Angelegenheiten der Strafgerichtsbarkeit regelt, lediglich in ihrem Anwendungsbereich auf Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der – nunmehr auch ausdrücklich angeführten – weisungsfreien Justizverwaltung beschränkt.

Außerdem wird die Bestimmung begrifflich an die Terminologie der DSGVO („justizielle Tätigkeit“) angepasst.

Zu § 85a GOG:

Die Zulässigkeit der Verarbeitung von Daten durch Strafgerichte richtet sich grundsätzlich nach den Bestimmungen der StPO. Eine § 83 Abs. 1 GOG entsprechende ausdrückliche gesetzliche Grundlage der Berechtigung zur Verarbeitung soll in § 74 Abs. 1 StPO aufgenommen werden, um nicht nur Gerichte, sondern auch Staatsanwaltschaft und Kriminalpolizei zu erfassen.

Dem Begriff Angelegenheiten der Strafgerichtsbarkeit liegt ein weites Verständnis zugrunde. So ist eine Verarbeitung personenbezogener Daten nicht nur im Bereich der gerichtlichen Entscheidungstätigkeit, sondern auch in jenem der zur unabhängigen Rechtsprechung zählenden kollegialen Justizverwaltung (Art. 87 Abs. 2 B-VG) unter den durch § 74 Abs. 2 StPO normierten Prämissen zulässig. Ebenso erfasst ist die Tätigkeit der im Gerichtsverfahren bestellten Sachverständigen und Dolmetscher.

Einer § 84 GOG idgF entsprechenden Bestimmung bedarf es für den Bereich der Strafgerichtsbarkeit nicht. Die den angeführten Bestimmungen der Verordnung (EU) 2016/679 entsprechenden Regelungen der DS-RL wurden im Wesentlichen durch §§ 43 bis 45 DSG idF BGBl. I. Nr. 120/2017 umgesetzt. Sie umfassen die Verpflichtung des Verantwortlichen zur Information sowie die Rechte der betroffenen Person auf Auskunft, Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung. Hierbei handelt es sich um Pflichten bzw. Rechte, hinsichtlich derer spezielle, auf die besondere Stellung und Funktion des Strafverfahrens abstellende Regelungen in der StPO bestehen. Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (leges speciales) den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. So sind etwa insbesondere die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten als leges speciales zum 3. Hauptstück des DSG zu betrachten. Informationsverpflichtungen sind etwa in § 50, § 138 Abs. 5, § 139 Abs. 2 StPO zu ersehen, wobei diese im Einklang mit der für das Strafverfahren wesensimmanenten Zielsetzung der Aufklärung von Straftaten und Verfolgung verdächtiger Personen (§ 1 Abs. 1 StPO) unter Wahrung der Rechte Verdächtiger bzw. Beschuldigter auch dem Umstand einer möglichen Gefährdung des Zwecks des strafrechtlichen Ermittlungsverfahrens Rechnung tragen. Die Auskunft innerhalb der StPO wird typischerweise über die Regelung der Akteneinsicht präzisiert. Daneben bleibt kein Raum für das Auskunftsrecht nach dem DSG (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 60). In diesem Sinn führt auch der Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 23 aus, dass § 44 Abs. 5 DSG idF BGBl. I. Nr. 120/2017 die bisherige Regelung des § 26 Abs. 8 DSG 2000 übernimmt, wodurch klargestellt wird, dass das Auskunftsrecht wie bisher nicht zur Umgehung von in Materiengesetzen geregelten speziellen Einsichtsrechten (z.B. Akteneinsicht) herangezogen werden kann. In § 75 StPO finden sich ferner ausdrückliche Vorschriften über das Berichtigen, Löschen und Sperren personenbezogener Daten. Dort,

wo es an entsprechenden Regelungen in der StPO fehlt, finden gemäß § 74 Abs. 1 StPO die Bestimmungen des DSG subsidiär im Strafverfahren Anwendung.

§ 85 GOG kommt aufgrund seiner Ausgestaltung als subsidiärer Rechtsschutz nur dort zum Tragen, wo die StPO für die Durchsetzung der Datenschutzrechte keine ausreichenden Instrumente vorsieht. Der Anwendungsbereich der Bestimmung ist im Strafverfahren daher denkbar klein, weil typischerweise nach der StPO mit Einspruch wegen Rechtsverletzung, Beschwerde oder Nichtigkeitsbeschwerde/Berufung gegen das Urteil vorgegangen werden kann, um Datenschutzverletzungen geltend zu machen. Erst wo diese Möglichkeiten enden, ist das GOG einschlägig (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 67). Die durch das Strafprozessrechtsänderungsgesetz 2013, BGBl. I Nr. 195/2013, entfallene Befristung der Einbringungsmöglichkeit eines Einspruchs wegen Rechtsverletzung gemäß § 106 StPO mit Beendigung des Ermittlungsverfahrens hat zu einer weiteren Verkleinerung des Anwendungsbereichs des § 85 GOG geführt. Dessen ungeachtet dient die Bestimmung (etwa im Bereich der Geschäftsregister) nach wie vor dazu, dort Lücken im Rechtsschutz zu schließen, wo die Verfahrensordnung einen solchen nicht bietet. Aus diesem Grund wird die Geltung des § 85 GOG auch auf Strafgerichte erweitert.

Zu Z 3 und 4 (§ 89f GOG):

Die vorgeschlagenen Regelungen betreffen terminologische Anpassungen an die DSGVO. Das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz ist als Verantwortlicher für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten im Justizressort – neben der Abwicklung des Strafvollzuges und der Führung der zivil- und strafgerichtlichen Verfahren zählen hierzu nun insbesondere auch die vor dem Bundesverwaltungsgericht geführten Verfahren – verantwortlich. Es hat insbesondere sicherzustellen, dass die Sicherheit und Vertraulichkeit von personenbezogenen Daten hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können (Art. 5 DSGVO). Die hierzu erforderlichen technischen und organisatorischen Rahmenbedingungen sind der Bundesrechenzentrum GmbH als Auftragsverarbeiterin nach den Erfordernissen des Einzelfalls, insbesondere nach Maßgabe der Art der verarbeiteten personenbezogenen Daten und dem Einsatzgebiet der Verarbeitungstätigkeit, vom Verantwortlichen vorzugeben.

Zu Z 5 (§§ 89p und 89q GOG):

Zu § 89p GOG:

Art. 26 DSGVO beschäftigt sich mit dem Fall, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Datenverarbeitung festlegen. Diese sind dann als gemeinsam Verantwortliche im Sinne der DSGVO zu betrachten. Art. 26 DSGVO ermöglicht in diesen Fällen die gesetzliche Festlegung einer Verteilung der Aufgaben des Verantwortlichen, insbesondere was die Wahrnehmung der Rechte der von der Verarbeitung betroffenen Personen angeht.

Mit dem vorgeschlagenen § 85p wird zunächst zum Ausdruck gebracht, dass im Rahmen der justiziellen Tätigkeit in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen und der in Senaten zu erledigenden Justizverwaltung das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz und das jeweils verfahrensführende Gericht gemeinsam als für die Verarbeitung Verantwortliche nach Art. 26 DSGVO zu betrachten sind. Geregelt wird auch die Aufgabenverteilung der datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitung. Soweit nicht gesondert eine gerichtliche Zuständigkeit vorgesehen ist, treffen die Rechte und Pflichten des Verantwortlichen das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. Diese (Auffang-)Zuständigkeit ergibt sich aus dem Umstand, dass die technische Struktur der von den verfahrensführenden Gerichten verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellten Applikationen (derzeit die Verfahrensautomation Justiz [VJ]) vorgegeben wird. Demnach sollen die Pflichten des Verantwortlichen im Umfang der Vorgaben der DSGVO (etwa gemäß Art. 24, 25 sowie 28 ff. DSGVO) das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz treffen.

Entsprechend der im vorgeschlagenen § 84 GOG getroffenen Einschränkung der Anwendbarkeit der Art. 12 bis 22 und 34 DSGVO kommt eine Aufgabenverteilung für diesen Bereich nicht mehr in Frage, weil hier bereits die Verfahrensvorschriften entsprechende (gerichtliche) Zuständigkeiten vorsehen. Daneben sehen die Verfahrensgesetze und das GOG punktuell eigene Zuständigkeiten für Auskunftsrechte außerhalb eines konkreten gerichtlichen Verfahrens vor. So ermöglicht etwa § 89l jedermann beim Bezirksgericht seines Wohnsitzes oder Aufenthalts ein Auskunftsrecht über Gericht und Aktenzahl aller im elektronischen Register enthaltenen zivilgerichtlichen Verfahren, in denen er Partei ist. Auch hier sieht das jeweilige Materiengesetz eine entsprechende (gerichtliche) Zuständigkeit vor.

Zu § 89q GOG:

Nach § 36 Abs. 2 Z 8 DSG idF BGBl. I. Nr. 120/2017 ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff ersetzt jenen des Auftraggebers nach § 4 Abs. 4 DSG 2000. Der Verantwortliche zeichnet für die Einhaltung der durch §§ 74 f StPO bzw. § 37 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 festgelegten Kriterien der Zulässigkeit einer Datenverarbeitung verantwortlich, ihn treffen unter Berücksichtigung der durch die StPO (das DSG) normierten Voraussetzungen die Pflichten zur Information, Auskunftserteilung, Berichtigung und Löschung personenbezogener Daten und Einschränkung deren Verarbeitung.

§ 47 DSG idF BGBl. I. Nr. 120/2017 sieht die Möglichkeit vor, dass die Verantwortlichkeit durch zwei oder mehrere Personen gemeinsam wahrgenommen wird. Aufgrund des Umstands, dass die Struktur der seitens des jeweils verfahrensführenden Gerichts verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellte Applikation Verfahrensautomation Justiz (VJ) vorgegeben wird, soll das jeweils fallbearbeitende Gericht gemeinsam mit dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz die Position des Verantwortlichen wahrnehmen. Entsprechend der von § 47 DSG idF BGBl. I. Nr. 120/2017 geforderten Vorgabe soll ausdrücklich normiert werden, dass die Wahrnehmung der Rechte und Pflichten des Verantwortlichen nach der StPO (aufgrund des Verweises in § 74 Abs. 1 StPO subsidiär des DSG) das jeweils verfahrensführende Gericht trifft. Zur Vermeidung der Notwendigkeit einer Befassung jedes einzelnen in Strafsachen tätigen Gerichts soll im Einklang mit der für den zivilgerichtlichen Bereich geltenden Bestimmung des § 89l GOG festgelegt werden, dass jede auskunftssuchende Person beim Haft- und Rechtsschutzrichter des für Strafsachen zuständigen Landesgerichts seines Wohnsitzes oder gewöhnlichen Aufenthalts eine bundesweite Auskunft über Gericht und Aktenzahl aller in der VJ enthaltenen strafgerichtlichen Haupt- und Rechtsmittelverfahren beantragen kann, in denen sie Beteiligte ist. Eine Auskunft über anhängige Ermittlungsverfahren darf jedoch selbst für den Fall, dass in einem solchen Verfahren eine Befassung des Haft- und Rechtsschutzrichters erfolgt ist, nicht erteilt werden, weil diese Verfahren unter Leitung der Staatsanwaltschaft – und nicht des Gerichts – stehen (§ 20 Abs. 1 StPO).

Zu Z 6 und 7 (§§ 91b und 91d GOG):

Die vorgeschlagenen Regelungen betreffen terminologische Anpassungen an die DSGVO.

Zu Z 8 (Inkrafttretens- und Übergangsbestimmungen)

Die Änderungen sollen gleichzeitig mit dem Inkrafttreten der DSGVO in Kraft treten. Übergangsbestimmungen sind lediglich für die §§ 84, 85 und 85a erforderlich.

Zu Artikel 6 (Änderung des GUG):

Zu Z 1 (§ 6a GUG):

Rechtsanwälte und Notare sind gemäß § 6 Abs. 2 GUG unter bestimmten Umständen zur direkten Abfrage des Personenverzeichnisses befugt: Notare, um als Gerichtskommissär in Verlassenschaftssachen oder als Erbenmachthaber verbücherte Rechte des Erblassers zu ermitteln (Z. 1); Rechtsanwälte, um als Erbenmachthaber verbücherte Rechte des Erblassers zu ermitteln und um Personen, die im Personenverzeichnis eingetragen sind, Abschriften und Mitteilungen über die sie betreffenden Eintragungen zu erteilen (Z. 1a); Notare und Rechtsanwälte, um als Vertreter des Gläubigers einer vollstreckbaren Geldforderung verbücherte Rechte des Schuldners zu ermitteln (Z. 1b). In den nach den genannten Bestimmungen nicht vorgesehenen Fällen haben auch Notare und Rechtsanwälte die Einsicht in das Personenverzeichnis nach § 5 Abs. 4 GUG bei Gericht zu beantragen und dafür ein rechtliches Interesse darzulegen.

In technischer Hinsicht gehen die Einsichtsmöglichkeiten der Rechtsanwälte und Notare aber über ihre gesetzlich vorgesehenen Einsichtsrechte hinaus. Der Entwurf sieht daher in der vorgeschlagenen Bestimmung einen Auskunftsanspruch über die Abfrage von Daten aus dem Personenverzeichnis durch Rechtsanwälte und Notare vor, damit die Betroffenen prüfen können, ob die Direktabfrage ihrer Daten aus dem Personenverzeichnis den Anforderungen des § 6 Abs. 2 GUG entsprach.

Die Auskunft ist beim Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz zu beantragen und von diesem zu erteilen, wenn der Antragsteller dartut, dass die Daten zur Einleitung oder Führung eines gerichtlichen, berufs- oder disziplinarrechtlichen Verfahrens benötigt werden. Diese Einschränkung soll zur Entlastung der Verwaltung dienen; eine Auskunft soll nur dann erteilt werden müssen, wenn beim Antragsteller gewisse Verdachtsmomente bestehen, dass eine unzulässige Abfrage des Personenverzeichnisses erfolgt sein könnte.

Gemäß § 6 Abs. 2 Z. 2 GUG sind auch die Dienststellen des Bundes, der Länder und der Gemeinden sowie die Sozialversicherungsträger und der Hauptverband der Sozialversicherungsträger zur Abfrage des Personenverzeichnisses befugt, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben notwendig ist. Die Zulässigkeit dieser Abfragen kann von der Justiz nicht überprüft werden; vielmehr muss dies im jeweiligen Wirkungsbereich der genannten Stellen geschehen. Folglich wird den betroffenen Personen in diesem Bereich ein entsprechendes Auskunftsrecht im GUG nicht eingeräumt.

Zu Artikel 7 (Änderung der JN):

Zu Z 1 (§ 37 Abs. 1a und 1b JN):

Das Ersuchen eines Gerichts um Übermittlung des Gerichtsakts eines anderen Gerichts ist ein Ersuchen um Rechtshilfe im Sinn des § 37 JN (SZ 57/161). So fasst auch die Geschäftsordnung für die Gerichte erster und zweiter Instanz die Aktenübersendung als Akt der Rechtshilfe auf, weshalb sie diese einer Regelung im Rahmen der „bürgerlichen Rechtshilfesachen“ (§§ 432 bis 436 Geo) unterzieht und anordnet, dass Ersuchen um Übersendung zivilgerichtlicher Akten in das Rechtshilferegister (Hc) einzutragen sind (§ 432 Abs. 1 Z 3 Geo). Die Aktenübersendung wird auch als häufigster Fall der – der Rechtshilfe vergleichbaren – Amtshilfe zwischen den Organen der Vollziehung (Art. 22 B-VG) genannt (6 Ob 656/84).

Die inländischen Gerichte sind einander gemäß § 37 Abs. 1 JN zur Rechtshilfe verpflichtet (vgl. Art 22 B-VG).

In Ausführung des Rechtshilfeersuchens ist das ersuchte Gericht zwar grundsätzlich an das Gesuch gebunden. Die Durchführung der Erledigung ist aber eine selbständige Amtshandlung des Rechtshilfegerichts und nicht der Kontrolle durch das Prozessgericht unterworfen (vgl. *Fasching* Zivilprozessrecht Lehr- und Handbuch Rz 316).

Aufgrund des Umstands, dass mittlerweile die Akteninhalte weitgehend in der Verfahrensautomation Justiz (VJ) gespeichert sind, besteht der Wunsch aus der richterlichen Praxis, eine gesetzliche Grundlage zu schaffen, damit der Weg der Beischaffung von Teilen oder Informationen aus einem anderen Gerichtsakt in bestimmten Fällen „abgekürzt“ werden kann und diese möglichst unmittelbar der elektronischen Aktenverwaltung der VJ entnommen werden können.

Mit dem vorgeschlagenen § 37 Abs. 1a JN soll eine entsprechende Rechtsgrundlage für eine unmittelbare elektronische Aktenbeischaffung unter der Voraussetzung zur Verfügung gestellt werden, dass das Gericht die für seine Entscheidung maßgeblichen Tatsachen von Amts wegen zu ermitteln hat. Außerdem hat es diesfalls den Vorgang der Beischaffung dem anderen Gericht in geeigneter Weise zur Kenntnis zu bringen, damit dieser Vorgang im beigeschafften Akt dokumentiert ist.

Die mit der vorgeschlagenen Bestimmung getroffenen Einschränkungen sind insbesondere aus datenschutz- und persönlichkeitsrechtlichen Erwägungen erforderlich. Mit der Beischaffung des Gerichtsakts eines anderen Gerichts ist notwendiger Weise ein Eingriff in die Rechtssphäre der an diesem Verfahren beteiligten Personen verbunden. Nach § 1 Abs. 2 letzter Satz DSG sowie nach Art. 5 Abs. 1 lit. c DSGVO darf ein Eingriff in das Grundrecht auf Datenschutz jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen werden. Die unmittelbare Beischaffung anderer Gerichtsakten soll demzufolge nur dann gestattet werden, wenn das Gericht zur amtswegigen Ermittlung verpflichtet ist, weil es sich in diesen Fällen in aller Regel um Verfahren mit Rechtsfürsorgecharakter handelt, in denen zum Wohl der geschützten Person fallbezogen ein rasches Handeln angezeigt sein kann. Außerdem sollen die Meldung der unmittelbaren Aktenbeischaffung und deren Dokumentation im beigeschafften Akt einerseits einem überschießenden Gebrauch von dieser Möglichkeit vorbeugen und andererseits die Parteien des anderen Verfahrens von dem Vorgang in Kenntnis setzen.

Auch die vorgeschlagene unmittelbare elektronische Aktenbeischaffung ist ein Fall der Rechtshilfe. Jedoch nimmt der Gesetzgeber durch die vorgeschlagene Bestimmung die Amtshandlung des ersuchten Gerichts vorweg, indem er die Rechtshilfe unter den gesetzlich festgelegten Voraussetzungen generell zulässt.

Mit dem vorgeschlagenen § 37 Abs. 1b JN soll der unmittelbaren elektronischen Aktenbeischaffung eine weitere Schranke gesetzt werden.

Stehen der Aktenübersendung oder Auskunftserteilung aus einem Akt Rechtsvorschriften entgegen, die die Rechtshilfe beschränken (wie etwa § 141 AußStrG), gebietet es in einer Interessensabwägung der Schutz der Interessen der Parteien dieses Verfahrens, eine unmittelbare Beischaffung des Aktes in solchen Fällen nicht zu gestatten. Dann obliegt es dem ersuchten Gericht, im „normalen“ Weg der Rechtshilfe zu entscheiden, ob und gegebenenfalls in welchem Umfang es eine Übermittlung von Akteninhalten an das ersuchende Gericht zulässt.

Damit eine solche Beschränkung der Aktenübersendung oder Auskunftserteilung sofort ersichtlich ist, sind die betreffenden Akten vom verfahrensführenden Gericht in der VJ entsprechend zu kennzeichnen.

Zu Z 2 (§ 37 Abs. 6 JN):

Bei Rechtshilfeersuchen eines ausländischen an ein inländisches Gericht (§§ 38, 39 und 40 JN) ist für den Fall der Verweigerung der Rechtshilfe oder bei sonstigen Meinungsverschiedenheiten zwischen dem ersuchenden und dem ersuchten Gericht ein Regulativ vorgesehen (§ 40 JN). Diesfalls hat auf Begehren des ersuchenden ausländischen Gerichts oder eines anderen hiezu berufenen ausländischen öffentlichen Organs das dem ersuchten Gericht vorgesetzte Oberlandesgericht über die Rechtmäßigkeit der Weigerung oder über den sonstigen Gegenstand der Meinungsverschiedenheit zu entscheiden.

Wird einem Ersuchen einer Staatsanwaltschaft um Amts- oder Rechtshilfe von einem ersuchten Gericht nicht oder nicht vollständig entsprochen, so hat das dem ersuchten Gericht übergeordnete Oberlandesgericht gemäß § 76 Abs. 2a StPO auf Antrag der Staatsanwaltschaft ohne vorhergehende mündliche Verhandlung über die Rechtsmäßigkeit der unterlassenen Amts- oder Rechtshilfe oder über den sonstigen Gegenstand der Meinungsverschiedenheit zu entscheiden.

Bei Streitigkeiten zwischen ersuchendem und ersuchtem (jeweils inländischen) Gericht über die Verweigerung der Rechtshilfe ist jedoch ein gerichtliches Verfahren nach geltendem Recht nicht ausdrücklich vorgesehen.

Mit der vorgeschlagenen Bestimmung soll diese Rechtschutzlücke geschlossen werden, indem in diesen Fällen § 40 JN sinngemäß anzuwenden sein soll. Zur Entscheidung über diese Streitigkeit ist das beiden Gerichten übergeordnete Gericht berufen.

Der rechtliche Charakter der Entscheidung über das zugrunde liegende Rechtshilfeersuchen kommt in der gewählten Verweisungsnorm (anders als in § 47 JN, welcher sich alternativ als mögliche Verweisungsnorm angeboten hätte) passend zum Ausdruck. Die Amtshilfe ist zwar ein Akt der Gerichtsbarkeit (6 Ob 656/84), hat aber bloß internen Charakter; weder die Verfahrensparteien noch das ersuchende Organ haben ein subjektives Recht darauf, dass Amtshilfe geleistet oder verweigert wird oder sind Partei in einem Verfahren zur Erlangung der Amtshilfe (vgl. 10 Ob 28/07a).

§ 40 JN eröffnet in sinngemäßer Anwendung einen direkten Rechtszug auf Antrag des ersuchenden Gerichts an das beiden Gerichten übergeordnete Gericht, und zwar in Form einer Beschwerde sui generis. Mit der Beschwerde sollen in der konkreten Rechtshilfesache strittig gewordene (Verfahrens-)Fragen ausjudiziert werden; diese können die (gänzliche oder teilweise) Verweigerung der Rechtshilfe, die Art ihrer Ausführung oder jede sonstige zwischen ersuchendem und ersuchtem Gericht ausgebrochene Meinungsverschiedenheit betreffen (vgl. *Sengstschmid* in *Fasching/Konecny*[3] § 40 JN Rz 1).

Zu Z 3 (§ 37a JN):

Zunächst darf auf die Erläuterungen zum vorgeschlagenen § 37 Abs. 1a und 1b JN verweisen werden.

Mit der vorgeschlagenen Bestimmung soll die in der gerichtlichen Praxis ebenfalls immer wieder strittige Frage geklärt werden, in welchen Fällen die von Verwaltungsbehörden (etwa den Gewerbebehörden, Finanzämtern, Kinder- und Jugendhilfeträgern ua) an ein Gericht gestellten Ersuchen um Amtshilfe durch Übersendung des Gerichtsaktes zulässig sind und in welchen Fällen diese verweigert werden dürfen.

Wie zum vorgeschlagenen § 37 Abs. 1a und 1b JN bereits ausgeführt, wird die Aktenübersendung als häufigster Fall der Amtshilfe zwischen den Organen der Vollziehung (Art. 22 B-VG) genannt.

Gemäß Art. 22 B-VG sind alle Organe des Bundes, der Länder und der Gemeinden im Rahmen ihres gesetzmäßigen Wirkungsbereichs zur wechselseitigen Amtshilfe verpflichtet. Zur Möglichkeit der Ausgestaltung dieser Verpflichtung durch einfaches Gesetz führt *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Rz 50 zu Art. 22 B-VG mit Verweis auf mehrere Belegstellen aus, es sei nahezu unbestritten, dass der Gesetzgeber Art. 22 B-VG näher ausgestalten, dh die Amtshilfe zwischen Organen und Gebietskörperschaften konkretisieren darf. Dem Gesetzgeber steht daher nicht nur die Erweiterung frei; er kann Amtshilfe auch beschränken (*Wiederin* aaO). Es ist überdies eine gesetzliche Grundlage in Konstellationen erforderlich, in denen das ersuchte Organ faktische Leistungen erbringen soll, die in Grundrechte eingreifen; Datenübermittlungen, die in Art. 8 EMRK oder in das Grundrecht auf Datenschutz eingreifen, müssen als Informationseingriffe gesetzlich zugelassen sein (*Wiederin* aaO Rz 51).

Vor diesem Hintergrund wird in der vorgeschlagenen Bestimmung die gesetzliche Verpflichtung von Gerichten, Amtshilfe auf Ersuchen inländischer Verwaltungsbehörden durch Übermittlung von Gerichtsakten oder von Teilen dieser zu leisten, dahingehend beschränkt, dass die begehrte Übermittlung nur soweit erfolgen darf, als diese auf einer ausdrücklichen gesetzlichen Grundlage beruht. Die

ersuchende Behörde hat die gesetzliche Grundlage für Übermittlung gegenüber dem ersuchten Gericht anzuführen.

Hintergrund dieser Regelung ist, dass es einer ausdrücklich vom jeweiligen Materiengesetzgeber getroffenen Wertungsentscheidung bedarf, in welchen Fällen das Informationsinteresse im Verfahren vor der ersuchenden Behörde das Geheimhaltungsinteresse im gerichtlichen Verfahren überwiegt.

Eine weitere Einschränkung der Verpflichtung zur Amtshilfe kann sich daraus ergeben, dass der Übermittlung bestimmter Informationen aus einem Gerichtsakt spezielle Rechtsvorschriften entgegenstehen, wie dies etwa für Auskünfte über Einkommens- und Vermögensverhältnisse oder Informationen zum Gesundheitszustand der vertretenen Person in Erwachsenenschutzverfahren der Fall ist (vgl. § 141 AußStrG).

Zu Artikel 8 (Änderung der Notariatsordnung):

Zu Z 1 (§ 37 Abs. 3a NO):

Das zu § 9 Abs. 3a RAO Gesagte gilt sinngemäß.

Zu Z 2 und 4 (§§ 134 Abs. 4 und 140a Abs. 3a NO):

Die vorgeschlagenen §§ 134 Abs. 4 und 140a Abs. 3a NO sehen – entsprechend den Anforderungen sowohl des europäischen wie auch des österreichischen Datenschutzrechts – vor, dass sowohl die Notariatskammern wie auch die Österreichische Notariatskammer personenbezogene Daten der Notare und Notariatskandidaten, die zur Erfüllung der jeweiligen gesetzlichen Aufgaben der Notariatskammer bzw. der Österreichischen Notariatskammer erforderlich sind, verarbeiten dürfen (wobei sich die Ermächtigung im Bereich der Notariatskammern auf die Daten der Mitglieder des jeweiligen Notariatskollegiums [vgl. § 124 NO], im Bereich der Österreichischen Notariatskammer hingegen auf alle österreichischen Notare und Notariatskandidaten bezieht). Durch den Verweis auf Art. 4 Z 2 DSGVO wird gleichzeitig klargestellt, dass unter dem Begriff „verarbeiten“ alle in der genannten Definition der DSGVO angeführten Verarbeitungsvorgänge zu verstehen sind.

Zu Z 3 (§ 140a Abs. 2 Z 11 NO):

Dabei handelt es sich um eine Anpassung an die neue Terminologie der DSGVO.

Zu Z 5 (§ 140b Abs. 7 NO):

Die Österreichische Notariatskammer ist gemäß § 140b NO ermächtigt, die darin genannten Register, Archive und Verzeichnisse zu führen.

Die speziellen und von privatrechtlichen Datenanwendungen abweichenden Zwecke der Datenverarbeitung im Zusammenhang mit der Führung einzelner der Register, Archive und Verzeichnisse gemäß § 140b NO erfordern es, dass (teilweise) von der genannten Öffnungsklausel des Art. 23 DSGVO Gebrauch gemacht wird, um einerseits den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen (Art. 23 Abs. 1 lit. i DSGVO) und andererseits die Durchsetzung zivilrechtlicher Ansprüche (Art. 23 Abs. 1 lit. j DSGVO) zu gewährleisten. Insoweit sollen sich nach der vorgeschlagenen Bestimmung die sich aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung nach den Vorschriften dieses Bundesgesetzes, des § 91c GOG und der nach § 140a Abs. 2 Z 8 NO erlassenen Richtlinien der Österreichischen Notariatskammer richten, zumal die genannten Vorschriften ein umfassendes und auf die jeweiligen Verarbeitungszwecke abgestimmtes Regulativ (auch der datenschutzrechtlichen Aspekte der betroffenen Register, Archive und Verzeichnisse) vorsehen. Dies betrifft folgende der in § 140b Abs. 1 NO genannten Datenanwendungen:

- das „Österreichische Zentrale Testamentsregister“ (ÖZTR),

- das „Treuhandregister des österreichischen Notariats“ (THR),

- das nach § 91d Abs. 2 GOG hoheitlich zu führende „Urkundenarchiv des österreichischen Notariats“ und

- das „Österreichische Zentrale Vertretungsverzeichnis“ (ÖZVV).

Das ÖZTR dient der Registrierung der Verwahrung der bei Gerichten, Notaren und Rechtsanwälten hinterlegten letztwilligen Anordnungen, Erbverträge, Vermächtnisverträge, Erb- und Pflichtteilsverzichtsverträge sowie weiteren Urkunden über sonstige Erklärungen auf den Todesfall (§ 140c Abs. 1 NO). Die Österreichische Notariatskammer hat die registrierten Daten bei Anfragen von Verlassenschaftsgerichten und öffentlichen Notaren als Gerichtskommissäre in Verlassenschaftssachen an diese und zu Kontrollzwecken an Gerichte, Notare und Rechtsanwälte auf deren Verlangen hinsichtlich der von ihnen gemeldeten Daten registrierungsfähiger Urkunden zu übermitteln (§ 140c Abs. 3 NO).

Das ÖZTR dient der Auffindbarkeit errichteter Testamente. Bis zum Wirksamwerden des registrierten Testaments dient die Registrierung ausschließlich dem Interesse des Testators. Rechte dritter Personen sind soweit nicht berührt, weshalb diesen auch keine Rechte nach Art. 12 bis 22 und 34 DSGVO zukommen können (und sollen). Mit dem Ableben des Testators ist es Aufgabe der im gerichtlichen Verlassenschaftsverfahren tätigen Organe (Gericht und Gerichtskommissär), allfällige registrierte Testamente abzufordern und gemäß den dann anzuwendenden Verfahrensvorschriften (insbesondere des AußStrG und des GKG) im Rahmen der justiziellen Tätigkeit abzuhandeln; diesfalls kommen die Bestimmungen über das gerichtliche Verfahren zur Anwendung.

Das THR dient der Registrierung der nach § 109a Abs. 2 NO eintragungspflichtigen Treuhandschaften. Einzutragen sind insbesondere der Notar, die Versicherung des Notars, der Treuhandrahmen, die Treugeber und der Beginn und das Ende der Treuhandschaft. Jeder Treugeber ist berechtigt, von der Österreichischen Notariatskammer darüber Auskunft zu verlangen, ob die ihn betreffende Treuhandschaft im THR registriert ist und in welcher Höhe dafür Versicherungsschutz besteht (§ 140d Abs. 1 und 2 NO).

Die §§ 109a und 140d NO und die auf der Grundlage der §§ 109a Abs. 5 und 140b Abs. 2 Z 8 NO ergangenen Richtlinien der Österreichischen Notariatskammer vom 8.6.1999 über die Vorgangsweise bei notariallen Treuhandschaften (THR 1999) enthalten insgesamt ein umfassendes Schutzregime insbesondere zur Absicherung des Treugebers, das auch dessen (über die DSGVO hinausgehenden) Auskunfts- und Informationsrechte im Detail regelt (vgl. etwa die Pkte. 27 ff. der THR 1999).

Das Urkundenarchiv des österreichischen Notariats dient der Speicherung von Notariatsakten oder dem Notar von den Parteien übergebenen Urkunden (§ 110 Abs. 1 NO). Zweck des Urkundenarchivs ist ferner die Speicherung von Urkunden, die für den elektronischen Urkundenverkehr mit den Gerichten bestimmt sind.

Das Urkundenarchiv dient insgesamt ausschließlich dem Schutz der Rechte der Parteien und (gegebenenfalls) der Durchsetzung ihrer zivilrechtlichen Ansprüche. Deren datenschutzrechtliche Sphäre ist durch die von der Österreichischen Notariatskammer nach § 140b Abs. 5 NO zu erlassenden Richtlinien sowie die anzuwendenden Verfahrensvorschriften geschützt. Den Parteien ist vom Notar elektronischer Zugang zu diesen Urkunden zu ermöglichen (§ 91c Abs. 3 GOG). Die Parteien sind berechtigt, in der in den Richtlinien vorgesehenen Form auch anderen Personen elektronischen Zugang zu diesen Urkunden einzuräumen. Außer den in diesem Gesetz angeführten Fällen darf ein Zugriff auf diese Urkunden nur über gerichtlichen Auftrag dem Gericht oder im Rahmen der standesrechtlichen Aufsicht über Auftrag der Notariatskammer dieser ermöglicht werden (§ 110 Abs. 3 NO).

Das ÖZVV ist in § 140h NO detailliert geregelt. Es dient insbesondere der Registrierung von Vorsorgevollmachten und (gemäß dem 2. Erwachsenenschutz-Gesetz, BGBl. I Nr. 59/2017, für Eintragungen ab dem 30.6.2018) von Vereinbarungen über eine gewählte Erwachsenenvertretung, von gesetzlichen Erwachsenenvertretungen, Erwachsenenvertreter-Verfügungen und gerichtlichen Erwachsenenvertretungen sowie von Kündigungen, Änderungen und Widerrufen der genannten Rechtsinstitute. Da in diesem Bereich sensible Daten der betroffenen Personen verarbeitet werden, bedarf es spezieller Rechtsschutzvorkehrungen, die in § 140h NO sowie den auf der Grundlage des § 140a Abs. 2 Z 8 NO ergangenen Richtlinien der Österreichischen Notariatskammer vom 4.6.2007 für das Österreichische Zentrale Vertretungsverzeichnis (ÖZVV-RL 2007), daneben aber auch in den anzuwendenden Verfahrensvorschriften insbesondere des AußStrG getroffen sind. Die angesprochenen Regelungen dienen ferner dem Schutz des Geschäftsverkehrs und damit – entsprechend der Öffnungsklausel des Art. 23 Abs. 1 lit. i DSGVO – der Sicherstellung der Rechte und Freiheiten anderer Personen.

Angesichts der dargestellten umfangreichen und spezifisch abgestimmten Schutzregime im Bereich der genannten Register, Archive und Verzeichnisse ist bei diesen jeweils die vorgeschlagene, auf Art. 23 Abs. 1 lit. i und j DSGVO beruhende datenschutzrechtliche Sonderregelung gerechtfertigt.

Mit der vorgeschlagenen Bestimmung soll überdies eine Verteilung der Aufgaben des Verantwortlichen im Sinn des Art. 26 DSGVO vorgenommen werden. Demgemäß treffen die Rechte und Pflichten des Verantwortlichen für die Datenverarbeitungen, soweit die diesbezüglichen Bestimmungen der DSGVO im Zusammenhang mit den jeweiligen Datenanwendungen des Notariats anwendbar sind, die Österreichische Notariatskammer, wenn nicht in diesem Bundesgesetz, in § 91c GOG oder in den nach § 140a Abs. 2 Z 8 erlassenen Richtlinien eine Zuständigkeit des einzelnen Notars angeordnet ist.

Zu Z 6 (§ 168 NO):

Das zu § 20 Abs. 4 und 5 DSt Gesagte gilt sinngemäß.

Zu Art. 9 (Änderung der Rechtsanwaltsordnung)

Zu Z 1 (§ 9 Abs. 3a RAO):

Das Gebot der anwaltlichen Verschwiegenheit zählt zu den tragenden Säulen des Anwaltsberufs. Das Recht auf – und damit verbunden – die Pflicht des Rechtsanwalts zur Verschwiegenheit ist unverzichtbares Kernelement der Rechtsstaatlichkeit und unerlässlich für den Zugang zum Recht und das Grundrecht auf ein faires Verfahren (*Manhart*, Verschwiegenheit und Doppelvertretung, AnwBl 2014, 161 mwN). Eine Anwaltschaft ohne streng verstandene Verschwiegenheitsverpflichtung ist nicht denkbar. Für die berufsmäßige Parteienvertretung durch Rechtsanwälte kommt dem Umstand besondere Bedeutung zu, dass sich Klienten darauf verlassen können, dass von Seiten des Rechtsanwaltes und seiner Mitarbeiter keinerlei Informationen an Dritte gelangen. Erst dieses Vertrauen ermöglicht die Offenheit des Klienten gegenüber seinem Rechtsanwalt, die erforderlich ist, damit seine Interessen bestmöglich gewahrt werden können.

Schutzobjekt des anwaltlichen Verschwiegenheitspflicht sind die Parteiinteressen. Jedermann, der sich in seinen Angelegenheiten an einen berufsmäßigen Parteienvertreter wendet, muss darauf vertrauen können, dass er nicht gerade durch Betrauung eines Parteienvertreters und Informationserteilung an diesen Beweismittel gegen sich schafft. Fehlt dieser Schutz, so fehlt ein wesentliches Element des Rechts, sich in seinen Angelegenheiten eines Rechtsbeistands zu bedienen (VfSlg. 10.291/1984; RIS-Justiz RS0116762; *Lehner* in *Engelhart/Hoffmann/Lehner/Rohregger/Vitek*, RAO[9] § 9 RAO Rz 24).

§ 9 Abs. 3 RAO stellt damit im Zusammenhang bereits bisher klar, dass dieses Recht des Rechtsanwalts auf Verschwiegenheit nicht (durch gerichtliche oder sonstige behördliche Maßnahmen) umgangen werden darf. In gleicher Weise dürfen aber auch die durch die DSGVO eingeräumten Rechte nicht dazu führen, dass es zu einer entsprechenden Umgehung kommt. Eben dies wird durch Art. 23 Abs. 1 lit. i und j DSGVO sichergestellt, der Beschränkungen der Rechte der betroffenen Personen im Sinn der Art. 12 ff. DS-GrundVO durch Rechtsvorschriften der Mitgliedstaaten dann zulässt, wenn diese Maßnahmen „den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“ oder „die Durchsetzung zivilrechtlicher Ansprüche“ sicherstellen.

Auf dieser Grundlage und diesen Überlegungen beruht der neu vorgeschlagene § 9 Abs. 3a RAO, der vorsieht, dass die Rechte der betroffenen Person nach der DSGVO nur dann und lediglich insoweit zur Anwendung kommen, als dem nicht das Recht des Rechtsanwalts auf Verschwiegenheit zum Schutz der Partei oder der Rechte und Freiheiten anderer Personen oder der Durchsetzung zivilrechtlicher Ansprüche entgegensteht. Dies ist deshalb notwendig, weil andernfalls die Gefahr bestünde, dass etwa der (Prozess-)Gegner einer zivilrechtlichen Streitigkeit im Weg des Informations- und Auskunftsrechts nach der DSGVO Auskünfte aus den Unterlagen und Akten des gegnerischen Rechtsanwalts erhalten könnte, die den Interessen der von diesem vetretenen Partei diametral entgegenstehen. Angesichts der Mannigfaltigkeit der hier möglichen Konstellationen ist gleichzeitig auch klar, dass eine generelle Beurteilung (und Anordnung) im Vorhinein, ob und inwieweit diese Beschränkung zum Tragen kommt, nicht möglich ist; dies ist gegebenenfalls vielmehr jeweils anhand der konkreten Umstände des Einzelfalls zu prüfen und zu bewerten.

Zu Z 2 und 4 (§§ 10a Abs. 8 und 36 Abs. 1 Z 4 RAO):

Das zu § 140b Abs. 7 NO Gesagte gilt für die Führung des Treuhandarchivs und des Urkundenarchivs durch die Rechtsanwaltschaft sinngemäß.

Die Führung des Treuhandarchivs ist im Bereich der Rechtsanwaltschaft insbesondere durch § 10a RAO sowie die nach § 27 Abs. 1 lit. g RAO von den Rechtsanwaltskammern für ihren jeweiligen Bereich erlassenen Richtlinien geregelt. Nach diesen Bestimmungen sollen sich nach dem Vorschlag daher auch die aus Art. 12 bis 22 und Art. 34 DSGVO sowie aus § 1 Abs. 3 DSG ergebenden Rechte und Pflichten sowie deren Durchsetzung richten.

Sonstige Rechte und Pflichten des Verantwortlichen für diese Datenverarbeitungen treffen den Österreichischen Rechtsanwaltskammertag, soweit nicht in diesem Bundesgesetz oder in den nach § 27 Abs. 1 lit. g RAO erlassenen Richtlinien eine Zuständigkeit des einzelnen Rechtsanwalts angeordnet ist.

Datenverarbeitungen zur Führung des Urkundenarchivs durch die Rechtsanwaltschaft sollen sich nach dem Vorschlag nach den Vorschriften dieses Bundesgesetzes, des § 91c GOG und der nach § 37 Abs. 1 Z 7 RAO erlassenen Richtlinien richten.

Auch für diese Datenverarbeitungen sollen die sonstigen Rechte und Pflichten des Verantwortlichen den Österreichischen Rechtsanwaltskammertag treffen, soweit nicht in diesem Bundesgesetz, in § 91c GOG oder in den nach § 37 Abs. 1 Z 7 RAO erlassenen Richtlinien eine Zuständigkeit des einzelnen Rechtsanwalts angeordnet ist.

Zu Z 3, 6 und 7 (§§ 23 Abs. 2a, 36 Abs. 1 Z 7 und 36 Abs. 6 RAO):

Das zu §§ 134 Abs. 4 und 140a Abs. 3a NO Gesagte gilt sinngemäß. Angesichts der von den Rechtsanwaltskammern einzurichtenden und aufrecht zu erhaltenden Einrichtungen zur Versorgung ihrer Mitglieder und deren Angehörigen ist die Ermächtigung zur Verarbeitung personenbezogener Daten sowohl im Bereich der Rechtsanwaltskammern als auch im Bereich des Österreichischen Rechtsanwaltskammertags ausdrücklich auch auf solche Daten allfälliger Anspruchsberechtigter oder Begünstigter aus den Versorgungseinrichtungen der Rechtsanwaltskammern zu beziehen.

Zu berücksichtigen ist ferner, dass die Rechtsanwälte und Rechtsanwaltsanwärter zwar jeweils Mitglieder „ihrer" Rechtsanwaltskammer, nicht aber auch Mitglieder des Österreichischen Rechtsanwaltskammertags sind. Angesichts dessen erscheint es aufgrund der dem Österreichischen Rechtsanwaltskammertag auch in Bezug auf die einzelnen Standesmitglieder gesetzlich zukommenden bzw. durch die Rechtsanwaltskammern gemäß § 36 Abs. 3 RAO übertragenenen Aufgaben geboten, die Erhebung personenbezogener Daten der Mitglieder der Rechtsanwaltskammern und allfälliger Anspruchsberechtigter oder Begünstigter aus den Versorgungseinrichtungen der Rechtsanwaltskammern sowie die Erfassung und Bereitstellung dieser Daten in einer Datenbank und deren Verwendung für die Zwecke der Versorgungseinrichtungen der Rechtsanwaltskammern ausdrücklich als Aufgabe des Österreichischen Rechtsanwaltskammertags zu definieren.

Zu Z 5 (§ 36 Abs. 1 Z 5 RAO):

Mit dem neu formulierten § 36 Abs. 1 Z 5 RAO soll die dem Österreichischen Rechtsanwaltskammertag nach dieser Bestimmung bereits jetzt implizit zukommende Befugnis zur Bereitstellung eines elektronischen Verzeichnisses der in die Listen der österreichischen Rechtsanwaltskammern eingetragenen Rechtsanwälte ausdrücklich klargestellt und als Aufgabe des Österreichischen Rechtsanwaltskammertags festgelegt werden. Sowohl dieses elektronische Anwaltsverzeichnis als auch das elektronische Verzeichnis für die Anwaltssignaturen (das zulässigerweise gemeinsam mit dem elektronischen Anwaltsverzeichnis geführt werden kann) müssen über die Website des Österreichischen Rechtsanwaltskammertags allgemein zugänglich sein.

Zu Artikel 10 (Änderung des StAG):

Zu Z 1 (§ 34a Abs. 2a StAG):

Siehe grundsätzlich die Erläuterungen zu Artikel 5 Z 3 (§ 85a GOG).

Da Staatsanwaltschaften aufgrund des Art. 90a B-VG als Organe der Gerichtsbarkeit anzusehen sind, kommt nach Auffassung des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz der in seiner geltenden Fassung auf eine Rechtsverletzung durch ein Organ der Gerichtsbarkeit abstellende § 85 GOG auch im staatsanwaltschaftlichen Bereich zur Anwendung (vgl. in diesem Sinn auch *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 63 zur alten Rechtslage mit dem Hinweis auf Burgstaller in *Korinek/Holoubek* [Hrsg], Österreichisches Bundesverfassungsrecht Art 90a B-VG Rz 21 und DSK vom 8. 5. 2009, K121.472/0003-DSK/2009/00 und vom 18. 11. 2009, K121.561/0004-DSK/2009, wonach Akte der aufgrund von Art. 90a B-VG als Organe der Gerichtsbarkeit anzusehenden Staatsanwaltschaften der Entscheidungsgewalt der DSK entzogen sind). Um den Anwendungsbereich der Bestimmung infolge deren vorgeschlagener Neufassung nicht einzuschränken, soll deren Regelungsgehalt nunmehr auch ausdrücklich in den – schon derzeit umfassten – staatsanwaltschaftlichen Bereich überführt werden.

Zu Z 2 (§ 34a Abs. 6 StAG):

Nach § 36 Abs. 2 Z 8 DSG idF BGBl. I. Nr. 120/2017 ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff ersetzt jenen des Auftraggebers nach § 4 Abs. 4 DSG 2000. Der Verantwortliche zeichnet für die Einhaltung der durch §§ 74 f StPO bzw. § 37 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 festgelegten Kriterien der Zulässigkeit einer Datenverarbeitung verantwortlich, ihn treffen unter Berücksichtigung der durch die StPO (des DSG) normierten Voraussetzungen die Pflichten zur Information, Auskunftserteilung, Berichtigung und Löschung personenbezogener Daten und Einschränkung deren Verarbeitung.

§ 47 DSG idF BGBl. I. Nr. 120/2017 sieht die Möglichkeit vor, dass die Verantwortlichkeit durch zwei oder mehrere Personen gemeinsam wahrgenommen wird. Aufgrund des Umstands, dass die Struktur der seitens der jeweils verfahrensführenden Staatsanwaltschaft verarbeiteten Daten zentral durch die vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz bereitgestellte Applikation Verfahrensautomation Justiz (VJ) vorgegeben wird, soll die jeweils fallbearbeitende Staatsanwaltschaft gemeinsam mit dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz die Position des Verantwortlichen wahrnehmen. Entsprechend der von § 47 DSG idF BGBl. I. Nr. 120/2017

geforderten Vorgabe soll ausdrücklich normiert werden, dass die Wahrnehmung der Rechte und Pflichten des Verantwortlichen nach der StPO (aufgrund des Verweises in § 74 Abs. 1 StPO subsidiär des DSG) ausschließlich die jeweils verfahrensführende Staatsanwaltschaft trifft.

Eine der Bestimmung des § 89q GOG vergleichbare Regelung soll es für den staatsanwaltschaftlichen Bereich hingegen nicht geben: Eine Auflösung des Spannungsverhältnisses zwischen dem Recht des Beschuldigten auf Information über das gegen ihn geführte Strafverfahren sowie seine wesentlichen Rechte einerseits und dem legitimen Geheimhaltungsinteresse der Staatsanwaltschaft bei Befürchtung, dass durch eine entsprechende Information ansonsten der Zweck der Ermittlungen gefährdet wäre, ist nur im Einzelfall durch eine den Geboten der Gesetz- und Verhältnismäßigkeit gemäß § 5 StPO Rechnung tragende Anwendung von § 50 Abs. 1 letzter Satz StPO auflösbar. Aus dem Wortlaut des § 50 Abs. 1 StPO („Information…darf nur so lange unterbleiben, als besondere Umstände befürchten lassen…“) ergibt sich, dass der Aufschub der Information des Beschuldigten restriktiv zu handhaben ist (*Achammer*, in *Fuchs/Ratz*, WK StPO § 50 Rz 5f). Jedenfalls ist der Beschuldigte vor bzw. unmittelbar nach der Ausübung von Zwang oder vor seiner Vernehmung zur Sache über den gegen ihn bestehenden Tatverdacht und seine Rechte aufzuklären (EBRV 25 BlgNR 22. GP 68f; *Pilnacek/Pleischl,* Das neue Vorverfahren, Rz 185; *Fabrizy*, StPO[13] § 50 Rz 2). Darüber hinaus unterliegt der Aufschub der Information des Beschuldigten im Wege des Einspruchs wegen Rechtsverletzung gemäß § 106 StPO der Kontrolle durch die unabhängigen Gerichte. Das durch den grundsätzlichen Zweck des Ermittlungsverfahrens bedingte Hindernis für eine aktive Verständigung des Beschuldigten darf nicht dadurch umgangen werden, dass dieser aktiv eine entsprechende Anfrage an eine oder mehrere nicht verfahrensführende Staatsanwaltschaften oder auch das Bundesministerium für Justiz richtet, weil schon mit einer Beantwortung einer solchen Anfrage dahin, „dass die Auskunft nicht erteilt werde“ bzw. „der begehrten Auskunft die Bestimmung des § 50 Abs. 1 dritter Satz StPO entgegen stehe“, der Zweck der Norm (nämlich die Geheimhaltung) vereitelt würde. Dasselbe gilt für einen Hinweis, an welche konkrete, nämlich verfahrensführende, Staatsanwaltschaft sich ein Auskunftswerber wenden solle. Im Ergebnis ist auch zur Vermeidung einer uneinheitlichen Praxis die begehrte Auskunft über die bei einer Staatsanwaltschaft gespeicherten personenbezogenen Daten oder dort anhängige Ermittlungsverfahren nur von der jeweils verfahrensführenden Staatsanwaltschaft zu erteilen, weil nur diese allein zur hinreichenden Beurteilung in der Lage ist, ob über solche Daten bzw. ein dort anhängiges Ermittlungsverfahren Auskunft erteilt werden kann.

Zu Z 3 (§ 42 Abs. 20 StAG):

Die Bestimmung regelt das Inkrafttreten.

Zu Artikel 11 (Änderung der StPO):

Zu Z 1, 4 und 5 (Eintrag zu § 74 im Inhaltsverzeichnis, Überschrift von § 74 und § 74 Abs. 1 StPO):

Gerichte, Staatsanwaltschaften, Finanzstrafbehörden, Sicherheitsbehörden und sonstige staatliche Behörden, die mit der Erfüllung von Aufgaben im Strafverfolgungsbereich zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit betraut sind, fallen im Rahmen ihrer Aufgabenerfüllung in den Anwendungsbereich der DS-RL.

Deren Umsetzung erfolgte mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017. In dessen 3. Hauptstück finden sich explizite Regelungen zur Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung (§§ 36ff).

Wie im Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 18 ausdrücklich klargestellt, gehen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. So sind etwa insbesondere die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten leges speciales zum 3. Hauptstück des DSG. Ebenso sind die Bestimmungen über die Aufgaben der Datenschutzbehörde nach § 32 DSG – zumindest in den Fällen der Z 4, 5 und 8 – im Bereich des Strafverfahrens nicht anwendbar, an deren Stelle stehen die entsprechenden Rechtsbehelfe der StPO (bzw. subsidiär des GOG), die gerichtlichen Rechtsschutz gewährleisten, zur Verfügung. Einer ausdrücklichen gesetzlichen Anordnung des im Bericht des Verfassungsausschusses dargelegten Vorrangs des strafprozessualen Rechtsschutzsystems gegenüber der Aufsicht durch die Datenschutzbehörde bedarf es nicht: Gemäß § 31 Abs. 1 erster Satz DSG wird die Datenschutzbehörde als nationale Aufsichtsbehörde für den in § 36 Abs. 1 DSG genannten Anwendungsbereich eingerichtet. Nach dieser Bestimmung ist die Datenschutzbehörde jedoch für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen

nicht zuständig. Diese Ausnahme beruht auf der verpflichtenden Vorgabe des Art. 45 Abs. 2 DS-RL, wodurch sichergestellt werden soll, dass die Unabhängigkeit der Gerichte im Rahmen ihrer rechtsprechenden Tätigkeit gewahrt bleibt, obwohl die Richtlinie selbst auch für die Tätigkeit der Gerichte gilt (vgl. EG 80 der DS-RL). Aufgrund der Ausnahme in § 31 Abs. 1 zweiter Satz DSG ist ein doppelter Rechtsschutz von vornherein ausgeschlossen, weil in diesem Bereich ausschließlich die Bestimmungen der Materiengesetze (StPO, GOG, StAG) zur Anwendung gelangen. Im Ergebnis gilt daher der bereits in der geltenden Fassung des § 74 Abs. 1 StPO zum Ausdruck kommende Grundsatz der lediglich subsidiären Geltung des DSG gegenüber der StPO (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 2 f; 63) auch weiterhin.

Entsprechend § 38 DSG ist die Verarbeitung personenbezogener Daten, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, wenn sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird. Es soll daher in Ergänzung der bestehenden Verpflichtung zur Beachtung des Grundsatzes der Gesetz- und Verhältnismäßigkeit in § 74 Abs. 2 StPO eine ausdrückliche gesetzliche Grundlage für die Zulässigkeit der Datenverarbeitung durch Kriminalpolizei, Staatsanwaltschaften und (Straf-)Gerichte in § 74 Abs. 1 StPO geschaffen werden. Die von diesen wahrzunehmenden Aufgaben werden im Wesentlichen durch § 1 Abs. 1 StPO bestimmt: Kriminalpolizei, Staatsanwaltschaften und Gerichte haben Straftaten aufzuklären, verdächtige Personen zu verfolgen und damit zusammenhängende Entscheidungen zu treffen. Ebenso erfasst ist die Tätigkeit der im Ermittlungs- oder Hauptverfahren durch die Staatsanwaltschaft oder das Gericht bestellten Sachverständigen und Dolmetscher. Die offene Formulierung berücksichtigt weiters, dass die Staatsanwaltschaft nicht nur im Ermittlungsverfahren als dessen Leiterin, sondern in weiterer Folge auch im Hauptverfahren als Beteiligte (§ 210 Abs. 2 StPO) tätig wird und ermöglicht ihr so auch in diesem Verfahrensstadium die Verarbeitung entsprechender personenbezogener Daten; gleiches gilt für die Tätigkeiten der Oberstaatsanwaltschaft in den Strafverfahren vor dem Oberlandesgericht (§ 21 Abs. 1 StPO) und der Generalprokuratur in den Strafverfahren vor dem Obersten Gerichtshof (§ 22 StPO). Für die Strafgerichte ist auf die ebenfalls vorgeschlagene Bestimmung des § 85a GOG zu verweisen, in der zur Konkretisierung der in § 74 Abs. 1 StPO vorgeschlagenen Formulierung auf die Angelegenheiten der Strafgerichtsbarkeit abgestellt wird. Diesem Begriff liegt ein weites Verständnis zugrunde, wodurch die Verarbeitung personenbezogener Daten nicht nur im Bereich der gerichtlichen Entscheidungstätigkeit, sondern auch in jenem der zur unabhängigen Rechtsprechung zählenden kollegialen Justizverwaltung (Art. 87 Abs. 2 B-VG) unter den durch § 74 Abs. 2 StPO normierten Prämissen zulässig ist. § 74 Abs. 1 StPO schafft auch eine Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten, weil die hierfür in § 39 DSG normierten Voraussetzungen sowohl in § 74 Abs. 1 als auch in Abs. 2 StPO Deckung finden.

Soweit Kriminalpolizei, Staatsanwaltschaften und Gerichte auch mit der Erfüllung anderweitiger Aufgaben betraut sind, unterliegen sie in Bezug auf diese Tätigkeiten nicht den Vorschriften des 3. Hauptstücks des DSG, sondern der DSGVO (zur Abgrenzung von Grenzfällen siehe den Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 17 f).

Die vorgeschlagene Änderung der Überschrift des § 74 StPO bezweckt eine Anpassung an die Terminologie des DSG idF BGBl. I. Nr. 120/2017.

Zu Z 3 (§ 54, § 76 Abs. 4 StPO):

Die vorgeschlagenen Änderungen betreffen Anpassungen von Verweisen an das DSG, inhaltliche Änderungen sind damit nicht verbunden. Durch die Änderung des DSG mit dem Datenschutz-Anpassungsgesetz 2018, BGBl. I. Nr. 120/2017, leitet sich der Begriff der „schutzwürdigen Geheimhaltungsinteressen“ nunmehr ausschließlich aus der unverändert gebliebenen Verfassungsbestimmung des § 1 Abs. 1 DSG ab.

Zu Z 2, 6, 7, 9 bis 11 und 13 bis 18 (Eintrag zu § 75 im Inhaltsverzeichnis, § 74 Abs. 2, Überschrift von § 75, § 75 Abs. 3 und 4, § 76 Abs. 4, § 117 Z 1, § 141 Abs. 1 und 4, § 142 Abs. 2 und § 143 Abs. 1 und 2 StPO):

Die vorgeschlagenen Änderungen der StPO stellen redaktionelle und terminologische Anpassungen an die neue Struktur und Terminologie des DSG idF BGBl. I. Nr. 120/2017 dar.

Zu Z 8 (§ 75 Abs. 1 StPO):

Die vorgeschlagenen Änderungen betreffen in erster Linie Anpassungen an die Terminologie des DSG idF BGBl. I. Nr. 120/2017.

Das Recht auf Berichtigung bzw. Vervollständigung personenbezogener Daten ist im Strafverfolgungskontext nur eingeschränkt durchsetzbar. Insbesondere sind davon keine nachträglichen Veränderungen von Aussagen bei Vernehmungen umfasst; hier bezieht sich die Richtigkeit und Vollständigkeit der personenbezogenen Daten auf die Übereinstimmung mit der Aussage selbst und nicht auf deren Inhalt (vgl. auch EG 47 der DS-RL bzw. den Bericht des Verfassungsausschusses 1761 BlgNR XXV. GP S. 23).

Während § 27 Abs. 1 DSG 2000 für die Berichtigung oder Löschung von Daten sowohl ein Antragsrecht (Z 1) als auch ein Vorgehen des Auftraggebers von Amts wegen (Z 2) vorsieht, findet sich in § 75 Abs. 1 StPO bislang keine entsprechende Regelung. Nach hA ist davon auszugehen, dass die Berichtigung entsprechend der Wertung des § 27 DSG 2000 sowohl von Amts wegen wie auch auf Antrag unverzüglich durchzuführen ist (*Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 75 Rz 1).

Zwar sieht § 45 Abs. 1 und 2 DSG idF BGBl. I. Nr. 120/2017 eine von § 27 Abs. 1 DSG 2000 abweichende Regelung dahingehend vor, dass ein Vorgehen von Amts wegen nur im Fall der Löschung von Daten, nicht jedoch bei einer bloßen Berichtigung möglich ist. Gleichwohl ergibt sich eine solche Verpflichtung aus § 37 Abs. 1 Z 4 iVm § 37 Abs. 3 DSG, weshalb dem jeweils verfahrensführenden Gericht oder der jeweils verfahrensführenden Staatsanwaltschaft als Verantwortlichem (siehe hierzu die vorgeschlagenen § 89q Abs. 2 GOG und § 34a Abs. 6 StAG) die Verpflichtung zur Löschung und Berichtigung von Daten von Amts wegen zukommen. Zur Verdeutlichung der sich aus verschiedenen Fundstellen des DSG schließenden Verpflichtungen wird vorgeschlagen, diese ausdrücklich in § 75 Abs. 1 StPO zu normieren.

Entsprechend § 45 Abs. 5 und 6 DSG idF BGBl. I. Nr. 120/2017 sollen von einer Berichtigung oder Löschung jene Behörden und Gerichte, denen diese personenbezogenen Daten übermittelt wurden (§ 76 Abs. 4 StPO) sowie von einer Berichtigung überdies jene Behörden und öffentlichen Dienststellen des Bundes, der Länder und der Gemeinden sowie andere durch Gesetz eingerichtete Körperschaften und Anstalten des öffentlichen Rechts, von denen die personenbezogenen Daten stammen, zu verständigen sein.

Zu Z 12 (§ 77 Abs. 2 StPO):

Die vorgeschlagene Neufassung des § 77 Abs. 2 StPO versteht sich als zentrale Grundlage der Zulässigkeit der Übermittlung personenbezogener Daten eines Strafverfahrens zu wissenschaftlichen Zwecken. Grundvoraussetzung der Anwendung ist, dass die Daten im Anwendungsbereich der DS-RL (entsprechend § 36 Abs. 1 DSG idF BGBl. I. Nr. 120/2017 somit zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung) ermittelt wurden.

Unter Berücksichtigung des § 40 Abs. 1 und 2 DSG idF BGBl. I. Nr. 120/2017, der grundsätzliche Vorgaben zur Zulässigkeit der Übermittlung solcher Daten zu wissenschaftlichen Zwecken innerhalb des Anwendungsbereichs der DS-RL (etwa zu Präventionszwecken) und eines – in der Praxis weit häufiger vorkommenden – Zwecks außerhalb davon regelt, soll zur umfassenden Wahrung der Datenschutzrechte betroffener Personen eine Übermittlung nur möglich sein, wenn eine Pseudonymisierung (§ 36 Abs. 2 Z 5 DSG idF BGBl. I. Nr. 120/2017 = „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“) personenbezogener Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist und überdies das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Geheimhaltungsinteresse der betroffenen Personen erheblich überwiegt. Wie auch bisher dürfen Daten ferner nur zum Zweck einer nicht personenbezogenen Auswertung für wissenschaftliche oder historische Forschungszwecke oder vergleichbare im öffentlichen Interesse liegende Untersuchungen (worunter auch Archivzwecke zu verstehen sind) übermittelt werden. Ungeachtet der den Empfänger der Daten im Regelfall treffenden Vorgaben der DSGVO ist von diesem auch weiterhin § 54 StPO zu beachten.

Aufgrund der künftig erforderlichen sorgfältigen Abwägung des vom Antragsteller hinreichend darzulegenden öffentlichen Interesses an der Forschungsarbeit einerseits und des schutzwürdigen Geheimhaltungsinteresses der betroffenen Personen andererseits soll den betroffenen Personen unter Berücksichtigung des Umstands, dass das öffentliche Interesse jenes auf Geheimhaltung erheblich zu überwiegen hat, die Auswertung ohnedies nur nicht personenbezogen erfolgen darf und der Empfänger als Verantwortlicher im Regelfall den umfassenden Verpflichtungen der Verordnung (EU) 2016/679 sowie überdies der Bestimmung des § 54 StPO unterliegt, das Recht auf Auskunft (§ 44 DSG idF

BGBl. I. Nr. 120/2017) nicht zukommen. Damit im Einklang treffen den verantwortlichen Übermittelnden auch keine Informationspflichten (§ 43 DSG idF BGBl. I. Nr. 120/2017). Der Ausschluss der Rechte der betroffenen Personen auf Information (§ 43 DSG) und auf Auskunft (§ 45 DSG) gründet auf Art. 15 Abs. 1 lit. e bzw. Art. 16 Abs. 4 lit. e der DS-RL (Freiheit der Wissenschaft nach Art. 17 StGG). Die Rechte der betroffenen Personen auf Berichtigung oder Löschung nach § 75 Abs. 1 StPO bleiben unberührt, jedoch sind diese im Zusammenhang mit einem Vorgehen nach § 77 Abs. 2 StPO ohnedies ohne Relevanz.

Zu Z 19 (§ 514 Abs. 37):

Die Bestimmung regelt das Inkrafttreten.

Zu Artikel 12 (Änderung des Strafregistergesetzes):

Zu Z 1 und 2 (§ 1 Abs. 2 und 3 StRegG):

In § 1 Abs. 2 StRegG soll die Klarstellung erfolgen, dass die Führung des Strafregisters von der Landespolizeidirektion Wien als Verantwortliche gemäß Art. 4 Z 7 iVm Art. 24 Datenschutz-Grundverordnung erfolgt.

Zudem ist beabsichtigt, – ohne eine materielle Änderung der Rechtslage herbeizuführen – im Sinne der Transparenz (vgl. Erwägungsgrund 39 zur Datenschutz-Grundverordnung) in § 1 Abs. 3 StRegG ausdrücklich festzulegen, dass der Bundesminister für Inneres die Funktion des Auftragsverarbeiters gemäß Art. 8 Z 8 iVm Art. 28 Abs. 1 Datenschutz-Grundverordnung ausübt. Darüber hinaus soll gesetzlich normiert werden, dass der Bundesminister für Inneres in dieser Funktion auch verpflichtet ist, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h Datenschutz-Grundverordnung wahrzunehmen, da andernfalls der Abschluss einer Vereinbarung über die Datenschutzpflichten erforderlich wäre (vgl. Art. 28 Abs. 3Datenschutz-Grundverordnung).

Zu Z 3 und 4 (§ 8 Abs. 1, 2 und 5 StRegG):

Das umfassende Recht auf Berichtigung, Löschung sowie Einschränkung der Verarbeitung personenbezogener Daten des Betroffenen ergibt sich aus der Datenschutz-Grundverordnung (vgl. Art. 16, 17 und 18). Gemäß Art. 23 ist es jedoch zulässig, diesbezügliche Pflichten und Rechte im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern zum einen eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und zum anderen in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Zudem muss die Beschränkung näher normierte wichtige Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates sicherstellen.

Da es sich bei den Strafregisterdaten um vor allem für Zwecke der Strafrechtspflege und inneren Sicherheit essentielle Daten handelt, ist eine Beschränkung der Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung aus Gründen der öffentlichen Sicherheit gemäß Art. 23 Abs. 1 lit. c Datenschutz-Grundverordnung, des Schutzes sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses gemäß Art. 23 Abs. 1 lit. e Datenschutz-Grundverordnung und des Schutzes der betroffenen Person gemäß Art. 23 Abs. 1 lit. i Datenschutz-Grundverordnung unbedingt erforderlich. Demzufolge sollen die genannten Rechte nur in Form eines spezifischen Feststellungsverfahrens wahrgenommen werden können. Da die Pflichten gegenüber dem Betroffenen nach der Datenschutz-Grundverordnung den Verantwortlichen treffen, soll künftig der Antrag bei der Landespolizeidirektion Wien einzubringen sein, die hierüber zu entscheiden hat. In Anbetracht der Tatsache, dass auf Basis der internen Aufzeichnungen des Bundesministeriums für Inneres in den vergangenen Jahren lediglich im Durchschnitt acht Anträge pro Jahr gestellt wurden, ist diesbezüglich für die Landespolizeidirektion Wien auch mit keinem erheblichen Mehraufwand zu rechnen. Der Betroffene soll demnach bei der Landespolizeidirektion Wien unter anderem die Feststellung beantragen können, dass die Aufnahme oder Nichtaufnahme einer Verurteilung oder einer sich darauf beziehenden Entschließung oder Entscheidung in das Strafregister zu Unrecht erfolgte. Das Rechtsschutzverfahren ermöglicht die Überprüfung der Zulässigkeit, Richtigkeit und Vollständigkeit einer Registereintragung durch die Landespolizeidirektion Wien. Das Verfahren dient jedoch nicht der Überprüfung eines Strafurteils oder einer darauf bezugnehmenden Gerichtsentscheidung (vgl. *Kert* in *Fuchs/Ratz*, WK-StRegG § 8 Rz 1 und 14).

Betreffend das Recht der betroffenen Person, vom Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wird darauf hingewiesen, dass im Verfahren nach § 8 StRegG auch die Feststellung beantragt werden kann, dass die Tilgung der Verurteilung nach dem TilgG (bereits) eingetreten ist. Ist dies der Fall, darf sie nicht mehr in der Strafregisterauskunft oder Strafregisterbescheinigung aufscheinen. Auch wenn dies das Gesetz nicht ausdrücklich vorsieht, kann laut höchstgerichtlicher Judikatur mit einem Antrag nach § 8 StRegG auch die Feststellung begehrt werden, dass eine Verurteilung der Beschränkung der Auskunft gemäß § 6 TilgG unterliegt (vgl. VwGH 99/01/0453).

Da sich der Anwendungsbereich der Art. 16 bis 18 Datenschutz-Grundverordnung mit jenem des § 8 StRegG deckt, soll es nicht erforderlich sein, dass sich der Betroffene in seinem Antrag gemäß § 8 StRegG auch noch zusätzlich auf die Datenschutz-Grundverordnung stützt.

Erst wenn dem Antrag nach Abschluss des Feststellungverfahrens ganz oder teilweise Folge gegeben wird, ist das Strafregister gemäß Abs. 3 zu berichtigen. Demzufolge kommt dem Feststellungsbescheid konstitutive Wirkung zu. Andererseits würden – sofern der Betroffene die Einschränkung der Verarbeitung verlangt (vgl. Art. 18 Abs. 1 lit. a Datenschutz-Grundverordnung) – die bestrittenen Daten bis zum Abschluss des Feststellungsverfahrens nicht im Strafregister aufscheinen, was insbesondere die Möglichkeit der Beurteilung der Vertrauenswürdigkeit von Personen (z.B. Sicherheitsüberprüfungen bzw. Gefährderprognosen) vollständig konterkarieren und eine Missbrauchsgefahr mit sich bringen würde. Die geplante Beschränkung hat auch kein Rechtsschutzdefizit zur Folge: Basis für die Eintragung bildet ein in einem rechtsstaatlichen Verfahren ergangenes rechtskräftiges Urteil, wobei der Betroffene bereits im Strafverfahren die Möglichkeit hatte, den Instanzenzug auszuschöpfen.

Das in Abs. 1 geregelte Rechtsschutzverfahren gegen Aufnahmen in das Strafregister soll – wie bisher – keine Anwendung auf Eintragungen rechtskräftiger Verurteilungen österreichischer Staatsbürger durch Strafgerichte anderer Mitgliedstaaten und die mit diesen Verurteilungen zusammenhängenden Informationen, die gemäß § 2 Abs. 1 Z 9 StRegG ausschließlich zum Zweck der Übermittlung eines Anhangs zu einer Strafregisterauskunft bereitgehalten werden, finden. Hinsichtlich der Aufnahme dieser Einträge in den Anhang kommt Österreich keine Auswahlbefugnis zu, auch deren Löschung richtet sich nach dem jeweiligen Recht des Urteilsstaates. Damit unterliegen die gemäß § 2 Abs. 1 Z 9 StRegG gespeicherten Einträge auch nicht dem Rechtsschutz des § 8 StRegG. Anträge auf Richtigstellung und Löschung hinsichtlich dieser Daten sind demnach an die zuständigen Behörden des Urteilsstaates zu richten (vgl. 1677 BlgNR 23. GP zu BGBl. I Nr. 29/2012).

Betreffend den Rechtsschutz gegen diesbezüglich erlassene Bescheide wird auf die Erläuterungen zu § 13c StRegG verwiesen.

Gemäß Art. 21 Abs. 1Datenschutz-Grundverordnung hat der Betroffene zudem das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten Widerspruch zu erheben. Ein solches, dem Betroffenen durch die Datenschutz-Grundverordnung in genereller Weise eingeräumtes Widerspruchsrecht kann jedoch gemäß Art. 23 Datenschutz-Grundverordnung zur Sicherstellung einer der in Abs. 1 lit. a bis j genannten Zwecke durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung wird in Abs. 5 für sämtliche nach dem StRegG verarbeiteten Daten Gebrauch gemacht.

Für einen geordneten Vollzug des StRegG sowie die Funktionalität des Strafregisters ist die Verarbeitung personenbezogener Daten in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 Datenschutz-Grundverordnung für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 Datenschutz-Grundverordnung vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene Person eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d Datenschutz-Grundverordnung). Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten von im Strafregister aufscheinenden Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (siehe auch Art. 23 Abs. 1 lit. h Datenschutz-Grundverordnung) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich.

Würde das Widerspruchsrecht zur Anwendung gelangen, würde dies dazu führen, dass eine Vielzahl der im Strafregister aufscheinenden Personen einer Verarbeitung der Verurteilungen widersprechen würden, was einen beträchtlichen Verwaltungsaufwand zur Folge hätte und den Vollzug wesentlich beeinträchtigen würde. Darüber hinaus könnten Verurteilungen – sofern die Betroffenen die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. d Datenschutz-Grundverordnung verlangen – erst dann in das Strafregister aufgenommen werden, wenn im jeweiligen Einzelfall abschließend geklärt wäre, dass die Interessen des Verantwortlichen an der Datenverarbeitung jenen des Betroffenen überwiegen. Im Falle eines Widerspruchs wäre nicht mehr gewährleistet, dass sämtliche strafrechtlich relevanten Daten tatsächlich im Strafregister aufscheinen, was den Zweck des Strafregisters – die

Evidenthaltung strafrechtlicher Verurteilungen zum Zwecke der Strafrechtspflege und inneren Sicherheit – vollständig konterkarieren würde. Weiters wäre im Falle eines Widerspruchs nach Art. 21 Datenschutz-Grundverordnung und der – wenn auch nur vorübergehenden – Unzulässigkeit einer Weiterverarbeitung nicht mehr gewährleistet, dass Gerichte oder sonstige Behörden sämtliche Daten und Informationen, die diese für eine rechtsrichtige Entscheidung sowie zu Strafbemessungszwecken benötigen, tatsächlich heranziehen können und könnte dies – vor allem bei Gefahr im Verzug (Gewalt in der Familie, notwendige Einstufung der Gefährlichkeit einer Person etc.) – in einer nicht zu unterschätzenden Verfahrensverzögerung resultieren.

Zu Z 5 bis 7 (§ 9 Abs. 1 Z 2a und 2b und § 9a Abs. 1 Z 5 und 6 StRegG):

Die Voraussetzungen für Übermittlungen personenbezogener Daten an Drittländer werden in Kapitel V Datenschutz-Grundverordnung festgelegt. Aus diesem Grund sollen die vorgeschlagenen Regelungen in § 9 und § 9a StRegG künftig differenzieren, je nachdem, ob sie Behörden aus Mitgliedstaaten der Europäischen Union oder Drittstaaten betreffen.

Hinsichtlich der Strafregisterauskünfte an Behörden aus Drittstaaten sowie Sonderauskünfte zu Sexualstraftätern an Gerichte, Staatsanwaltschaften und Sicherheitsbehörden aus Drittstaaten in Strafverfahren soll demzufolge betreffend die näheren Voraussetzungen lediglich ein Verweis auf die Datenschutz-Grundverordnung aufgenommen werden.

Zu Z 8 und 9 (§ 10 Abs. 1a und 4 StRegG):

Im Hinblick darauf, dass Auskünfte gemäß Art. 15 Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen (dazu gleich unten) und vor dem Hintergrund von Art. 12 Abs. 5 Datenschutz-Grundverordnung soll der letzte Satz in § 10 Abs. 1a StRegG entfallen.

Art. 23 Datenschutz-Grundverordnung ermächtigt die Union und die Mitgliedstaaten dazu, bestimmte Pflichten und Rechte, darunter auch das Auskunftsrecht gemäß Art. 15 Datenschutz-Grundverordnung, durch „Gesetzgebungsmaßnahmen“ zu beschränken, sofern gewisse näher normierte Gründe vorliegen (siehe auch die Erläuterungen zu § 8 StRegG). Diese Bestimmung enthält somit eine Öffnungsklausel, die einer gesetzlichen Maßnahme der Mitgliedstaaten zugänglich ist. Zum Schutz des Betroffenen (vgl. Art. 23 Abs. 1 lit. i Datenschutz-Grundverordnung) soll das Recht auf Auskunft insoweit gesetzlich beschränkt werden, als Auskünfte gemäß Art. 15 Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen.

Mit der Tilgung der Verurteilung erlöschen alle nachteiligen Folgen, die kraft Gesetzes mit der Verurteilung verbunden sind. Ist eine Verurteilung getilgt, so gilt der Verurteilte fortan als gerichtlich unbescholten und ist auch nicht verpflichtet, die getilgte Verurteilung anzugeben (vgl. § 1 TilgG). Das Strafregister dient zwar in vielen Bereichen der Beurteilung der Verlässlichkeit einer Person, wie für die Ausübung gefahrengeneigter Tätigkeiten (zB Gebrauch von Waffen und Sprengmitteln). Mit der Tilgung der Verurteilung soll es dem Verurteilten jedoch ermöglicht werden, nach einer gewissen Zeit des Wohlverhaltens wieder die Stellung eines Unbestraften zu erhalten. Sie soll demzufolge die Gefahr hintanhalten, dass frühere Verurteilungen, die bereits lange Zeit zurückliegen, bekannt werden und eine Wiedereingliederung des Täters in die Gesellschaft und die Arbeitswelt be- und verhindern (vgl. *Kert* in *Fuchs/Ratz*, WK-TilgG Vor Rz 5ff). Das Instrument der Auskunftsbeschränkung gemäß § 6 TilgG bietet ebenfalls den Vorteil, dass durch die weitgehende Einschränkung der Publizität der Verurteilungen die Resozialisierung des Täters erleichtert wird. Sie soll dem Betroffenen ermöglichen, gegenüber Dritten als unbescholten auftreten zu können. Nur dort, wo es die öffentliche Sicherheit erfordert, soll eine Auskunft über alle Verurteilungen gegeben werden, wie dies z.B. gegenüber Gerichten, Staatsanwaltschaften, Sicherheitsbehörden sowie bestimmten anderen Behörden der Fall ist. Der Verurteilte ist nicht verpflichtet, die Verurteilung gegenüber Behörden oder Privaten anzugeben.

Durch die Aufhebung der Regelung in § 26 Abs. 9 DSG 2000, wonach für Auskünfte aus dem Strafregister die besonderen Bestimmungen des StRegG über Strafregisterbescheinigungen gelten, durch das Datenschutz-Anpassungsgesetz 2018 würde die Gefahr bestehen, dass z.B. Dienstgeber oder andere Stellen die oben erwähnten Auskunftsbeschränkungen dadurch umgehen, dass anstelle einer Strafregisterbescheinigung die Beibringung eines Auskunftsbegehrens über sämtliche verarbeitete Daten gemäß Art. 15 Datenschutz-Grundverordnung verlangt wird. Das Telos von Tilgung und Auskunftsbeschränkung, dh Beseitigung der Stigmatisierung und Erleichterung der Resozialisierung, würde demnach ins Leere gehen. Dem soll die Regelung in § 19 Abs. 4 StRegG entgegenwirken, indem zum Schutz des Betroffenen Auskünfte gemäß Art. 15 Datenschutz-Grundverordnung in Form einer Strafregisterbescheinigung ergehen sollen und somit wie bisher weder getilgte Verurteilungen (§ 1 Abs. 5 TilgG) noch Verurteilungen, die einer Auskunftsbeschränkung unterliegen (§ 6 Abs. 4 TilgG), in diese Auskunft aufgenommen, noch darin auf irgendeine Art ersichtlich gemacht werden dürfen.

In Bezug auf die Ablehnungsgründe in Abs. 3 ist darauf hinzuweisen, dass auch die Datenschutz-Grundverordnung den Identitätsnachweis des Betroffenen zur Inanspruchnahme seiner Rechte als zulässig erachtet (vgl. Art. 12 Abs. 6 bzw. EG 64 Datenschutz-Grundverordnung). Der Antrag ist auch dann abzulehnen, wenn nach dem Antragsteller zum Zwecke der Aufenthaltsermittlung, Verhaftung oder Festnahme gefahndet wird. Der Bestimmung liegt die Überlegung zugrunde, dass es rechtspolitisch nicht vertretbar erscheint, dass derselbe Staat, der nach einer Person, die sich einer im Inland anhängigen Strafverfolgung oder -vollstreckung offenbar zu entziehen versucht, fahndet, derselben Person einen untadeligen Lebenswandel bescheinigt (ErläutRV 817 BlgNR 11. GP 11). Der Einschränkung liegt demnach ein wichtiges Ziel des allgemeinen öffentlichen Interesses gemäß Art. 23 Abs. 1 lit. e Datenschutz-Grundverordnung zugrunde.

Art. 12 Abs. 5 Datenschutz-Grundverordnung gilt gleichermaßen. Betreffend den Rechtsschutz gegen einen ablehnenden Bescheid wird auf die Erläuterungen zu § 13c StRegG verwiesen.

Zu Z 10 bis 14 und 22 (§ 10a Abs. 1 und 3, § 10b Abs. 1 und 2, § 11 Abs. 6 und § 14a Abs. 1 StRegG):

Sofern im Hinblick auf das neue Datenschutzregime eine Anpassung der im StRegG verwendeten Begriffe erforderlich erscheint, werden diese nun an die Definitionen der Datenschutz-Grundverordnung (Art. 4) angeglichen. Der Begriff der „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Z 2 Datenschutz-Grundverordnung beinhaltet auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung und entspricht damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff des „Verwendens“ bzw. der „Verwendung“ personenbezogener Daten.

Zudem sollen im Sinne der neuen datenschutzrechtlichen Terminologie beispielsweise die Begriffe „Übersendung“, „Mitteilung“, „Bekanntgabe“ oder „Weiterleitung“ von Daten durch das Wort „Übermittlung“ ersetzt werden.

Zu Z 15 und 16 (§ 12 StRegG):

§ 14 DSG 2000 sieht unter anderem vor, dass Protokolldaten über tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen drei Jahre lang aufbewahren sind, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird. Infolge des Entfalls des bisherigen § 14 DSG 2000 durch das Datenschutz-Anpassungsgesetz 2018 und den Umstand, dass die Datenschutz-Grundverordnung von spezifischen Regelungen betreffend die Protokollierung Abstand nimmt, wird vorgeschlagen, den – für Zwecke der Sicherheitspolizei einschlägigen – § 50 DSG, wonach aus den Protokolldaten auch die Identität eines allfälligen Empfängers verarbeiteter personenbezogener Daten hervorgehen muss, auf die Protokollierung von Datenverarbeitungsvorgängen im Rahmen des Strafregisters für anwendbar zu erklären. Die bisherige in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren soll vor dem Hintergrund der in der Datenschutz-Grundverordnung normierten Grundsätze der Datenminimierung gemäß Art. 5 Abs. 1 lit. c Datenschutz-Grundverordnung und der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e Datenschutz-Grundverordnung dem Zweck der Verarbeitung angepasst und somit auf zwei Jahre reduziert werden.

Zu Z 17 (§ 13a StRegG):

Aus datenschutzrechtlichen Überlegungen soll in § 13a Abs. 1 StRegG zum Schutz des Betroffenen die Klarstellung erfolgen, dass die Daten zu wissenschaftlichen Zwecken in einer Weise zu übermitteln sind, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen dem Empfänger nicht zur Verfügung stehen (vgl. die Begriffsbestimmung in Art. 4 Z 5 Datenschutz-Grundverordnung) und dieser die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Werden personenbezogene Daten zu wissenschaftlichen Zwecken verarbeitet, so können bei Vorliegen näher bestimmter Voraussetzungen gemäß Art. 89 Abs. 2 Datenschutz-Grundverordnung – vorbehaltlich der Bedingungen und Garantien gemäß Abs. 1 – durch nationales Recht Ausnahmen von den Rechten gemäß Art. 15 (Auskunftsrecht der betroffenen Person), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) vorgenommen werden. Da es in der Praxis kaum möglich wäre, gegenüber Betroffenen bei wissenschaftlichen Erhebungen aufgrund der hohen Datenmengen sämtliche dieser Rechte zu wahren bzw. die Wahrung der Betroffenenrechte die Verwirklichung der spezifischen wissenschaftliche Zwecke ernsthaft beeinträchtigen, wenn nicht sogar unmöglich machen würde, soll die Ausnahmeermächtigung gemäß Art. 89 Abs. 2 Datenschutz-Grundverordnung in Anspruch genommen werden.

Hinsichtlich der Informationspflicht gemäß Art. 14 Datenschutz-Grundverordnung („Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden“) wird – was den Vollzug betrifft – auf Art. 14 Abs. 5 Datenschutz-Grundverordnung verwiesen, wonach die Bestimmungen im Einzelfall insbesondere dann keine Anwendung finden, wenn und soweit sich die Erteilung dieser Information als unmöglich erweisen oder einen unverhältnismäßigen Aufwand erfordern würde, wie dies z.B. für die Verarbeitung für im öffentlichen Interesse liegende wissenschaftliche Zwecke der Fall sein kann. Jedenfalls sind aber vom Verantwortlichen geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu ergreifen (vgl. Art. 14 Abs. 5 lit. b Datenschutz-Grundverordnung). Diesbezüglich wird beispielsweise auf Abs. 1 hingewiesen, wonach der Empfänger der Daten aufgrund der vorgenommenen Pseudonymisierung keine Rückschlüsse auf die Identität des Betroffenen ziehen kann.

Im Sinne der neuen datenschutzrechtlichen Terminologie soll ferner der Begriff der „Bekanntgabe“ durch jenen der „Übermittlung“ ersetzt werden.

Zu Z 18 bis 20 (§ 13c StRegG):

Art. 54 Abs. 1 Datenschutz-Grundverordnung erlegt den Mitgliedstaaten auf, die in den lit. a bis f genannten Vorgaben durch Rechtsvorschriften im nationalen Recht vorzusehen. § 18 Abs. 1 DSG setzt in diesem Sinne die Datenschutzbehörde als einzige nationale Aufsichtsbehörde gemäß Art. 51 Datenschutz-Grundverordnung fest. Mit Geltung der Datenschutz-Grundverordnung, dh ab 25. Mai 2018, soll die bestehende Datenschutzbehörde somit die Funktion der nationalen Aufsichtsbehörde gemäß Art. 51 Datenschutz-Grundverordnung übernehmen.

Daraus ergibt sich, dass im Zuständigkeitsbereich der Datenschutz-Grundverordnung, dh für Beschwerden gegen sämtliche Feststellungsbescheide gemäß § 8 StRegG sowie gegen ablehnende Bescheide gemäß § 10 Abs. 4 StRegG, nicht ein Landesverwaltungsgericht, sondern – weil immer auch Rechte nach der Datenschutz-Grundverordnung betroffen sind – die Datenschutzbehörde zuständig ist, weshalb eine Anpassung der Regelung zu erfolgen hat. Damit soll zudem einer Parallelstruktur von Datenschutzbehörde und Landesverwaltungsgerichten entgegengewirkt werden. Zudem soll die Ergänzung erfolgen, dass die Landespolizeidirektion Wien in der betreffenden Rechtssache verpflichtet ist, den der Rechtsanschauung der Datenschutzbehörde entsprechenden Rechtszustand herzustellen und somit die Auskunft zu erteilen bzw. die Berichtigung, Löschung oder Einschränkung der Verarbeitung vorzunehmen hat.

Zu Z 12 (§ 14 Abs. 14 StRegG):

Die Bestimmung regelt das Inkrafttreten.

Zu Artikel 13 (Änderung des Strafvollzugsgesetzes):

Zu Z 1 (§§ 9 Abs. 5, 10 Abs. 1, 13, 14 Abs. 1 und 3, 14a Abs. 1, Abs. 2 Z 2 und Abs. 3, 15c Abs. 1, 16a Abs. 1 Z 2 und 3, 24 Abs. 3, 52 Abs. 3, 69 Abs. 1, 78 Abs. 1 und 2, 80 Abs. 2, 84 Abs. 1 und 3, 97, 101 Abs. 2 und 3, 106 Abs. 3, 116 Abs. 1, 121 Abs. 5, 121b Abs. 4, 134 Abs. 1 und 6, 135 Abs. 2, 161 sowie 179a Abs. 1 und 3 StVG), 5 (§§ 18a Abs. 3, 99 Abs. 5a und 156b Abs. 2 StVG), 6 (§ 156b Abs. 3 StVG) und 8 (§ 182 StVG):

Mit den vorgeschlagenen Änderungen soll die Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017, soweit hier relevant, nachvollzogen werden. Dies betrifft vor allem die Erweiterung des Bundesministeriums für Justiz zum Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. Im Bereich der Vollziehungsbestimmung des § 182 StVG ist überdies nunmehr sowohl hinsichtlich der Arbeit der Strafgefangenen (§§ 44 bis 55 StVG) und der sozialen Fürsorge (§§ 75 bis 84) als auch hinsichtlich der ärztlichen Betreuung (§§ 66 bis 74) und der Unterbringung in Anstalten für geistig abnorme Rechtsbrecher sowie in Anstalten für entwöhnungsbedürftige Rechtsbrecher (§§ 164 bis 170 StVG) gegebenenfalls das Einvernehmen mit dem Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz herzustellen.

Zu Z 2 (§ 15a StVG):

Abs. 1 bildet die Rechtsgrundlage für die Verarbeitung (bisher: Verwendung) personenbezogener Daten (§ 38 DSG idF BGBl. I Nr. 120/2017), einschließlich der bisher als „sensible Daten“ bezeichneten „besonderen Kategorien personenbezogener Daten“ im Sinne des § 39 DSG idF BGBl. I Nr. 120/2017 in Bezug auf die Insassen der Justizanstalten. Nach der zuletzt genannten Bestimmung ist die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person für u.a. die Zwecke der Verhütung von Straftaten sowie der Strafvollstreckung zwar

zulässig, jedoch nur dann, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden. Überdies muss die Verarbeitung – sofern sie sich nicht auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat – nach § 38 DSG idF BGBl. I Nr. 120/2017 zulässig sein; dies bedeutet, dass die Verarbeitung der personenbezogenen Daten grundsätzlich gesetzlich vorgesehen, für die Erfüllung einer Aufgabe wie der Verhütung von Straftaten oder der Strafvollstreckung erforderlich und verhältnismäßig sein muss. § 15a Abs. 1 übernimmt diese Kautelen.

Abs. 2 erfasst alle jene Personen, bei denen – abgesehen von den in Abs. 1 geregelten Insassen der Justizanstalten – die Verarbeitung personenbezogener zur Erfüllung der Aufgaben der Vollzugsverwaltung erforderlich sein kann (§ 38 DSG idF BGBl. I Nr. 120/2017). Dieses Erfordernis kann sich situationsbedingt (z.B. aus Anlass einer Besichtigung oder im Rahmen der Z 4), aber auch bei grundsätzlich länger andauerndem Kontakt zu einem Insassen oder der Vollzugsverwaltung ergeben (z.B. regelmäßige Besuche, Zulieferer). Soweit die betroffenen Personen die Anstalt betreten, kann auch die Verarbeitung biometrischer Daten, die zu den besonderen Kategorien personenbezogener Daten nach § 39 DSG idF BGBl. I Nr. 120/2017 zählen, erforderlich sein. Abs. 2 berücksichtigt gleichfalls die Kautelen der §§ 38 und 39 DSG idF BGBl. I Nr. 120/2017.

Abs. 3 regelt die Aufteilung der Aufgaben und Pflichten der gemeinsamen Verantwortlichen. Hinsichtlich zentraler Datenanwendungen, die den Vollzugsbehörden erster Instanz vom Bundesministerium für Justiz zur Nutzung zur Verfügung gestellt/vorgegeben und im Wege eines bundesweit einheitlich vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz herangezogenen Auftragsverarbeiters infrastrukturell (Hardware, Software, Applikationen) betreut werden (zB IVV, IWV etc.), werden die Pflichten des Verantwortlichen nach den §§ 46 DSG idF BGBl. I Nr. 120/2017 (Art. 24 DSGVO Abs. 1 und Abs. 2 [technische und organisatorische Datenschutzmaßnahmen] bzw. Art. 25 Abs. 1 und Abs. 2 [Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen]), § 49 DSG idF BGBl. I Nr. 120/2017 (Verzeichnis der Verarbeitungstätigkeiten), § 52 DSG idF BGBl. I Nr. 120/2017 (Datenschutz-Folgenabschätzung) und 54 DSG idF BGBl. I Nr. 120/2017 (Datensicherheitsmaßnahmen) vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz wahrgenommen. Die zentralen Datenanwendungen werden in den Verzeichnissen der Verarbeitungstätigkeiten sowohl des Bundesministeriums für Justiz als auch der Vollzugsbehörden erster Instanz aufgenommen. Andere, von den Vollzugsbehörden erster Instanz lokal betriebene Datenanwendungen sind zusätzlich in deren Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Die Wahrnehmung der Pflichten der Verantwortlichen hinsichtlich jener Datenanwendungen, die die Vollzugsbehörden erster Instanz aus eigenem lokal betreiben, obliegt den Justizanstalten. Ebenso obliegt den Vollzugsbehörden erster Instanz hinsichtlich sämtlicher Datenanwendungen (zentrale und insbesondere lokale Datenanwendungen) die Wahrnehmung der Rechte der betroffenen Personen nach den §§ 42 bis 45 DSG idF BGBl. I Nr. 120/2017 (das sind iW Informations- und Auskunftsrechte sowie gegebenenfalls das Recht auf Richtigstellung oder Löschung bzw. Einschränkung der Verarbeitung).

Die Abs. 4 und 5 entsprechen iW den bisherigen Abs. 3 und 4, wobei an die Stelle des bisherigen „Dienstleisters“ der „Auftragsverarbeiter“ und an die Stelle des „Auftraggebers“ der „Verantwortliche“ tritt.

Zu Z 3 (§ 15b StVG):

Da das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz Kompetenzen als oberste Vollzugsbehörde wahrnimmt (§ 13 StVG), während die AnstaltsleiterInnen Vollzugsbehörden erster Instanz sind (§ 11 StVG), soll die Differenzierung wo nicht sachlich geboten aufgehoben und stattdessen der einheitliche Begriff „Vollzugsbehörden“ verwendet werden. Die Erweiterung der Datenübermittlungsstellen um jenen „kraft Vereinbarung“ soll dem Umstand Rechnung tragen, dass im Forschungskontext in vertragliche Vereinbarungen mit externen Forschungspartnern üblicherweise auch Datenverarbeitungsvorgaben festgelegt werden. Mit dem letzten Satz des Abs 1 soll eine den Aktualitätsvorgaben des § 37 Abs. 1 Z 4 und Abs. 6 DSG idF BGBl. I Nr. 120/2017 entsprechende Regelung in das StVG aufgenommen werden.

Abs. 2 dient der „Umsetzung“ des § 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017 für die Zwecke des Strafvollzuges (vgl. für die Strafverfolgung die Ausführungen in den Gesetzesmaterialien zum Datenschutz-Anpassungsgesetz 2018, 1664 BlgNR XXV. GP, 19 = 1761 BlgNR XXV. GP, 31 f.). im Strafvollzugskontext kann sich ein entsprechender Anwendungsfall etwa bei der Weiterverarbeitung der aus Anlass des ersten Vollzuges einer Straf- oder Untersuchungshaft aufgenommenen Insassendaten für eine im unmittelbaren Anschluss nachfolgende Straf- oder Untersuchungshaft, sei es durch die datenerstverarbeitende Vollzugsbehörde oder eine z.B. im Wege der Klassifizierung (§ 134 StVG) oder Strafvollzugsortsänderung (§ 10 StVG, § 183 StPO) neu zuständige Vollzugsbehörde. Zur

Rechtsgrundlage für eine Weiterverarbeitung vormalig verarbeiteter Insassendaten im Falle neuerlicher Inhaftierung nach zwischenzeitiger Enthaftung oder Entlassung siehe Art. X Z 4 des Entwurfs(§ 15c Abs.3).

Abs. 3 entspricht im Wesentlichen dem geltenden Abs. 2. Unter einem dient diese Bestimmung auch als Grundlage für die Verarbeitung der von des Sicherheitsbehörden im Rahmen ihrer Zuständigkeit gem. § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 verarbeiteten Personendaten durch die Vollzugsbehörden für ihre im Rahmen des § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 notwendigen Zwecke (§ 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017).

Abs. 4 entspricht mit umgekehrten Vorzeichen der Regelung des Abs 3. Wird eine Person von der Vollzugsverwaltung an eine Sicherheitsbehörde oder eine sicherheitsbehördliche Hafteinrichtung übergeben, gründet die datenschutzrechtliche Verarbeitungszuständigkeit auf § 40 Abs. 1 DSG idF BGBl. I Nr. 120/2017. Nun existiert zwar bereits eine vergleichbare Bestimmung in Form des § 58b Abs 3 SPG. Da aber Insassen aus Justizanstalten nach ihrer justiziellen Anhaltung oftmals zu *fremden*polizeilichen Haftzwecken, deren Datenverarbeitungsgrundlage in der DSGVO gründet (und nicht durch die Zwecke des § 36 Abs. 1 DSG idF BGBl. I Nr. 120/2017 abgedeckt scheint), an die polizeilichen Behörden übergeben werden, soll für die Zulässigkeit der Datenübermittlung aus der Sphäre der Vollzugsbehörden in die Sphäre der Fremdenbehörden im Sinne des § 40 Abs. 2 DSG idF BGBl. I Nr. 120/2017 eine ausdrückliche gesetzliche Grundlage geschaffen werden.

Zu Z 4 (§ 15c StVG):

§ 15c regelt idgF den eingeschränkten Datenzugriff bzw. die Löschung von Insassendaten. Insoweit kann die Bestimmung im Wesentlichen unverändert bleiben. Es soll lediglich eine Löschungsvorschrift hinsichtlich der verarbeiteten personenbezogener Daten jener Personen, die keine Insassen sind (siehe dazu bei § 15a Abs. 2 StVG in der Fassung des Entwurfs), angefügt werden, die unter Berücksichtigung des sachlichen und verfahrensökonomischen Bedarfes der Vollzugsverwaltung – und § 37 Abs. 1 Z 5 DSG idF BGBl. I Nr. 120/2017 entsprechend – gestaffelt festgesetzt werden sollen.

Zu Artikel 14 (Änderung der ZPO):

Zu § 219 ZPO:

Mit der vorgeschlagenen Bestimmung soll die Umschreibung der im „öffentlichen Interesse“ zu berücksichtigenden Aspekte im Zuge der gemäß § 219 Abs. 2 ZPO zu treffenden Interessensabwägung an die in Art. 23 Abs. 1 DSGVG getroffene Wertung angepasst werden.