Der neue Datenschutz

Symposium
am 20. April 2018

Landesgruppe Österreich
der Internationalen Strafrechtsgesellschaft (AIDP)
und
Österreichischer Juristenverband

Für die Unterstützung
danken wir
dem Bundesministerium für Verfassung, Reformen,
Deregulierung und Justiz sowie
dem Österreichischen Juristenverband

Medieninhaber:
Landesgruppe Österreich
der Internationalen Strafrechtsgesellschaft
(AIDP)
A-1011 Wien, Justizpalast

Redaktion:
Mag. Dr. Andrea Lehner
(Universitätsassistentin post-doc, Universität Wien)
Mag. Michael Leitner
(Generalanwalt in der Generalprokuratur)

Druck:
Bundesministerium für Justiz
1070 Wien, Neustiftgasse 2

2019

Inhaltsverzeichnis

Vorwort

Prof. Dr. Otto F. Müller
Präsident der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft AIDP

Die Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) hat gemeinsam mit dem Juristenverband am 20.4.2018 im Palais Trautson ein Symposium zum Thema "Der neue Datenschutz" durchgeführt.

Die Vortragenden über das höchst aktuelle Symposiumsthema waren die Vortragenden Frau Prof. Dr. Eva Souhrada-Kirchmayer (Richterin am Bundesverwaltungsgericht) sowie die Herren Univ.-Ass. Dr. Roland Pichler (Universität Wien), Dr. Gerald Ganzger (Rechtsanwalt in Wien) und Mag. Kenan Ibili (Richter im auch für die Justiz zuständigen Bundesministerium), die unter der Leitung von Herrn Vizepräsidenten Prof. Dr. Ernst Eugen Fabrizy den zahlreichen Veranstaltungsteilnehmern auch zu einer lebhaften Diskussion zur Verfügung standen.

In Vertretung des Herrn Bundesministers Dr. Josef Moser sprach Herr Sektionschef Dr. Gerhard Hesse einleitend zum Symposiumsthema.

Unser besonderer Dank gilt allen am Podium Mitwirkenden und Herrn Sektionschef Dr. Gerhard Hesse für die Unterstützung durch das für die Justiz zuständige Bundesministerium und dem Juristenverband.

Wien, im April 2019

Einleitende Worte

Prof. Dr. Otto F. Müller
Präsident der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft AIDP

Sehr geehrte Damen und Herren!
Liebe Kolleginnen und Kollegen!

Es freut mich sehr, Sie im Namen der beiden Veranstalter, nämlich der österreichischen Landesgruppe der Internationalen Strafrechtsgesellschaft (AIDP) und des Juristenverbandes, repräsentiert durch dessen Präsidenten RA Prof. Dr. Fritz Wennig, begrüßen zu dürfen und Ihnen für Ihre Teilnahme an diesem Symposium herzlich zu danken, das ich damit auch eröffne. Unser besonderer Gruß gilt dem Herrn Sektionschef Dr. Gerhard Hesse, der den verhinderten Herrn Bundesminister Dr. Josef Moser vertritt.

Herzlich willkommen heiße ich die Vortragenden am Podium, nämlich Frau Prof. Dr. Eva Souhrada-Kirschmayer (Richterin am Bundesverwaltungsgericht) sowie die Herren Univ.-Ass. Dr. Roland Pichler (Universität Wien), Dr. Gerhard Ganzger (Rechtsanwalt in Wien) und Mag. Kenan Ibili (Richter in dem für die Justiz zuständigen Bundesministerium), die unter der bewährten Leitung unseres Vizepräsidenten Prof. Dr. Ernst Eugen Fabrizy auch zur Diskussion zur Verfügung stehen werden.

Gestatten Sie mir einige kurze Bemerkungen zum Tagungsthema, ohne den Vortragenden vorzugreifen.

Anlass für das heutige Symposium ist die aktuelle, ab 25.5.2018 wirksame, umfangreiche Neuregelung des Datenschutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten, vor allem durch die Datenschutzgrundverordnung des Europäischen Parlaments und des Rates vom 27.4.2016 und in deren Durchführung durch

ergänzende Regelungen durch das österreichische Datenschutz-Anpassungsgesetz 2018 vom 31.7.2017, BGBl I Nr. 120/2017.

In der Datenschutzgrundverordnung werden im Art 4 Z 1–26 zahlreiche Begriffsbestimmungen angeführt, wie etwa in Z 1, wonach unter "personenbezogenen Daten" alle Informationen verstanden werden, die sich auf eine identifizierte oder identifizierbare natürliche Person als "Betroffene Person" beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einer oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;"

Eine gleichlautende Definition findet sich im § 36 Abs 2 Z 1 des Datenschutzgesetzes im 3. Hauptstück mit der Überschrift "Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, des Strafvollstreckung und des Maßnahmenvollzugs".

Im Übrigen enthalten Art 4 der Datenschutzgrundverordnung und § 36 des Datenschutzgesetzes zahlreiche weitere wesentliche Begriffsbestimmungen, wie etwa betreffend ein Unternehmen, den Verantwortlichen, Auftragsverarbeiter und Datenschutzbeauftragten.

In Art 68 wird der Europäische Datenschutzausschuss zur Wahrung und Kontrolle des Datenschutzes definiert, dem auch der Leiter einer Aufsichtsbehörde jedes Mitgliedstaates und der Europäische Datenschutzbeauftragte angehören.

Im Datenschutzgesetz werden in den §§ 14–35 der Datenschutzrat und die Datenschutzbehörde mit ihren Aufgaben und Befugnissen angeführt, die nach § 35 Abs 1 nach den näheren Bestimmungen der Datenschutzgrundverordnung und dieses Bundesgesetzes zur Wahrung des Datenschutzes berufen ist.

Im § 27 Abs 1–5 wird das Verfahren über die Beschwerde an das Bundesverwaltungsgericht geregelt.

Im § 29 Abs 1 und 2 des Datenschutzgesetzes wird die Haftung und das Recht auf Schadenersatz gegen den Verantwortlichen oder Auftragsverarbeiter geregelt.

Umfang und Inhalt der angeführten Neuregelungen mit gegenseitigen Verweisungen (die Datenschutzgrundverordnung umfasst 99 Artikel auf 88 Seiten; das Datenschutzgesetz hat 70 §§ auf 35 Seiten) sowie mehrere Richtlinien und geplante weitere Anpassungsbestimmungen stellen hohe Anforderungen an die Erfüllung der umfangreichen organisatorischen und bürokratischen Aufgaben an alle Rechtsanwender wie etwa alle betroffenen Personen, Unternehmen, Verantwortliche, Auftragsverarbeiter, Datenschutzbeauftragte und zuständigen Behörden und Gerichte.

Dazu kommt die Pflicht zur erforderlichen umfassenden Information und Aufklärung über die neuen Datenschutzbestimmungen durch die dafür zuständigen und verantwortlichen Personen, denn die Datenschutzrechte wurden erheblich verbessert und erweitert, wie beispielweise bezüglich des Datenschutzbeauftragten, der Einwilligungshandlung der betroffenen Person, des Koppelungsverbotes, der Auskunftsrechte der Betroffenen, der Verpflichtung zur Löschung bestimmter Daten oder einer regelmäßigen Risikobewertung (Datenschutzfolgenabschätzung).

Als Strafrechtsgesellschaft haben wir auch besonderes Interesse an der Kenntnis von Sanktionen für Verstöße gegen die angeführten Gesetze.

Die Datenschutzgrundverordnung enthält keine strafgerichtlichen Bestimmungen, wohl aber im Art 83 "Allgemeine Bedingungen für die Verhängung von Geldbußen" für vorsätzliche oder fahrlässige Verstöße; für die Bemessung der Höhe der Geldbuße sind die in Art 83 Abs 2 lit a bis k und Abs 3 angeführten Umstände maßgeblich.

So ist gemäß Art 83 Abs 4 bei den in lit a bis c angeführten Verstößen eine Geldbuße bis zu 10.000.000 Euro oder im Falle eines Unternehmens bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vorgesehen.

Gemäß Abs 5 des Art 83 ist bei Verstößen gegen die in lit a bis e und der in Abs 6 angeführten Nichtbefolgung einer Anweisung der Aufsichtsbehörde eine Geldbuße bis zu 20.000.000 Euro oder im Fall eines Unternehmens bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vorgesehen.

Das Datenschutzgesetz enthält im 4. Hauptstück mit dem Titel "Besondere Strafbestimmungen" in § 62 Abs 1 Z 1–5 angeführte Taten, welche als Verwaltungsübertretung mit einer Geldstrafe bis zu 50.000 Euro bedroht sind, sofern die Tat nicht den Tatbestand nach Art 83 Datenschutzgrundverordnung verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

Gemäß Abs 5 ist die Datenschutzbehörde für die Entscheidung nach Abs 1 bis 4 zuständig.

§ 63 sieht die Bestrafung der Datenverarbeitung in Gewinn- oder Schädigungsabsicht unter den dort angeführten Voraussetzungen, sofern die Tat nicht nach einer anderen

Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen vor.

In beiden Strafbestimmungen ist die Subsidiaritätsklausel zu beachten.

Ebenso zu beachten sind hiebei die Strafbestimmungen des StGB, das in § 74 Abs 2 bestimmt, dass unter Daten im Sinne des StGB sowohl personenbezogene und nicht personenbezogene Daten als auch Programme zu verstehen sind.

Im § 126 a StGB wird die Datenbeschädigung mit Freiheitsstrafe bis zu 5 Jahren geahndet.

§ 225a StGB betrifft die Datenfälschung, die mit Freiheitsstrafe bis zu 1 Jahr oder mit Geldstrafe bis zu 720 Tagessätzen bestraft wird.

In § 226 StGB ist die tätige Reue geregelt.

Abschließend soll auch der Hinweis auf die bisher bekannt gewordene Kritik an den neuen Regelungen nicht verschwiegen werden.

Ich danke für Ihre Aufmerksamkeit und darf nun Herrn Sektionschef Dr. Gerhard Hesse um das Wort bitten.

Der neue Datenschutz (Schwerpunkt Datenschutz-Grundverordnung)[1]

Prof. Dr. Eva Souhrada-Kirchmayer[2]
Bundesverwaltungsgericht

1. Einleitung

Am 25. Mai 2018 wurde die Datenschutz-Grundverordnung[3] wirksam und trat das DSG in der Fassung des Datenschutz-Anpassungsgesetzes 2018[4] und weiteren zwei DSG-Novellen[5] in Kraft. Mit dem DSG wurde auch die Richtlinie 2016/680 (RL für die Polizei und Justiz in Strafsachen)[6] umgesetzt.

Schon in den Monaten davor überschlugen sich diesbezüglich die Meldungen. Während in der Wirtschaft manche Unternehmen bereits im Mai 2017 die „Panik" ausriefen,[7] versuchten andere zu beschwichtigen.[8] Handelt es sich bei diesen Rechtsinstrumenten um eine Revolution oder um eine

---

[1] Es handelt sich um die aktualisierte Fassung eines Vortrages, der am 20. April 2018 bei der AIDP gehalten wurde. Die Internet-Zitate beziehen sich auf den Stichtag 22. Mai 2018.
[2] Die Autorin ist stellvertretende Kammervorsitzende und Richterin am Bundesverwaltungsgericht und Vorsitzende der ESA-Datenschutzbehörde.
[3] Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119, 1.
[4] BGBl. I 120/2017.
[5] BGBl. I 23/2018 und BGBl I 24/2018.
[6] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 119, 89.
[7] Ein Jahr bis zur DSGVO, so Wirtschaftskammer: Panik? Panik! 21.05.2017, Business Recht Tech, https://extrajournal.net/2017/05/31/ein-jahr-bis-zur-dsgvo-so-wirtschaftskammer-panik-panik/.
[8] Keine Panik: Die EU-Datenschutzgrundverordnung kommt, https://www.bdsg-externer-datenschutzbeauftragter.de/behoerde/keine-panik-die-eu-datenschutzgrundverordnung-kommt/.

Evolution? fragen etwa die Professoren Kühling und Martini.[9] Ist es nicht einfach „more of the same“, wie etwa Prof. Forgó meint?[10]

Doch worum geht es überhaupt?

Vom europäischen „Gesetzgeber“ wurden zwei Datenschutzinstrumente beschlossen, wobei die Verordnung teilweise, die Richtlinie zur Gänze durch innerstaatliches Recht umzusetzen ist. Dies ist größtenteils durch das 2017 beschlossene „Datenschutzanpassungs-Gesetz 2018“ und die zwei genannten DSG-Novellen aus dem Jahr 2018 geschehen.

Der Vortrag dient dazu, einen kurzen Überblick über diese Rechtsinstrumente geben, wobei der Hauptfokus auf der Datenschutz-Grundverordnung (DSGVO) liegt. Die im Bereich der internationalen Strafrechtsgesellschaft ebenfalls sehr interessierende Richtlinie bzw. deren Umsetzung wird noch gesondert von meinen Kollegen am Podium näher beleuchtet werden. Allerdings kann man auch diese Richtlinie und deren Umsetzung nicht ohne die Bestimmungen der DSGVO verstehen, da sich auch die Richtlinie an dieser grundsätzlich orientiert und auch die österreichische Umsetzung zum Teil auf Bestimmungen der DSGVO Bezug nimmt.

2. Vorgeschichte der neuen Rechtsinstrumente[11]

Mit Inkrafttreten des Vertrags von Lissabon mit 1.12.2009[12] wurde mit Art 16 AEUV erstmals eine umfassende Rechtsgrundlage im Unionsprimärrecht für die Erlassung von Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und somit für die

[9] Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, *Jürgen Kühling/Mario Martini*, EuZW 2016, 448.
[10] Nikolaus Forgó am 21.11.2017 https://www.it-law.at/wp-content/uploads/2017/12/Forgo_Wien_it-law-symposion_112017.pdf.
[11] S dazu *Fercher/Riedl,* Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in: Knyrim (Hrsg), Datenschutz-Grundverordnung, Das neue Datenschutzrecht in Österreich und der EU (2016) 7 ff.
[12] ABl. C 306 vom 17.12.2007 S. 1 und ABl. C 115 vom 9.5.2008.

Erlassung von Rechtsakten auf dem Gebiet des Datenschutzes unter Einschließung des Bereichs der polizeilichen und justiziellen Zusammenarbeit in Strafsachen geschaffen.

Art 16 AEUV sieht vor, dass das Europäische Parlament (EP) und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr erlassen.

Die neue Rechtslage bot auf Unionsebene somit die Möglichkeit, ein ebenso zeitgemäßes wie den neuen primärrechtlichen Vorgaben nach Auflösung der Säulenstruktur durch den Vertrag von Lissabon angepasstes und einheitliches Datenschutzregime zu etablieren. Auch die Verbindlicherklärung der EU-Grundrechtecharta (GRC) und des Grundrechts auf Datenschutz in Art 8 GRC stellte einen maßgeblichen rechtlichen Faktor im Kontext der Neuregelung des unionsrechtlichen Datenschutzregimes dar.

Am 25.1.2012 legte die Europäische Kommission (EK) eine Mitteilung für eine Neuordnung des Datenschutzes auf Unionsebene vor, die auch zwei legislative Vorschläge umfasste, nämlich die genannte Verordnung und die genannte Richtlinie.

Nach mehrjährigen Verhandlungen, die sich vor allem in der Ratsarbeitsgruppe DAPIX („Data Protection and Information Exchange“) offenbar zäh gestaltete (während das Plenum des EP bereits am 12.3.2014 seinen Standpunkt in erster Lesung zur DSGVO beschlossen hatte, kam eine Beschlussfassung des Rates über den Standpunkt in erster Lesung zur DSGVO sowie zur Datenschutz-Richtlinie für den polizeilichen und justiziellen Bereich in Strafsachen erst am 8.4.2016 zustande), wurden die beiden Rechtsinstrumente schließlich nach mehr als

vier Jahren intensiver Verhandlungen am 27.4.2016 unterzeichnet. Österreich hat im schriftlichen Verfahren am 8.4.2016 gegen die DSGVO gestimmt, da aus österreichischer Sicht mehrere Problempunkte offengeblieben waren.

Die DSGVO wurde am 4.5.2016 kundgemacht. Sie trat am 20. Tag nach der Veröffentlichung in EU-Amtsblatt in Kraft und war ab dem 25.5.2018 anzuwenden.
Die Richtlinie für den polizeilichen und justiziellen Bereich in Strafsachen wurde ebenfalls am 4.5.2016 publiziert und trat einen Tag später in Kraft. Die Richtlinie war gemäß Art 63 bis zum 6.5.2018 umzusetzen. In der Abstimmung zur Richtlinie hat sich Österreich der Stimme enthalten.

3. Datenschutz-Anpassungsgesetz 2018

Die DSGVO ist als EU-Verordnung zwar prinzipiell direkt in den Mitgliedstaaten anwendbar und bedarf daher keiner grundsätzlichen Umsetzung, enthält aber – atypischer Weise – eine größere Zahl an „Öffnungsklauseln“ (Univ.-Prof. Jahnel hat 69 Öffnungsklauseln gezählt),[13] die – zumindest zum Teil zwingend – einer „Durchführung“ (Umsetzung) in den Mitgliedstaaten bedürfen. Insofern bestand ein innerstaatlicher Umsetzungsbedarf. Überdies war bis 6.5.2018 die RL (EU) 2016/680 umzusetzen.

Mit Datum 12.5.2017 wurde vom Bundeskanzleramt der Entwurf eines Datenschutz-Anpassungsgesetzes 2018 zur Begutachtung versendet. Als Ende der Begutachtungsfrist wurde der 23.6.2017 angegeben.

Ziel dieses Entwurfes war die tw. Umsetzung der DSGVO sowie die Umsetzung der RL (EU) 2016/680 sowie die Schaffung einer einheitlichen Kompetenz in den allgemeinen Angelegenheiten des Schutzes personenbezogener Daten, ein

[13] Dietmar Jahnel, Die DS-GVO und das DSG 2018 - Überblick und ausgewählte Fragestellungen, Vortrag gehalten am 22.2.2018 auf dem Internationalen Rechtssymposium (IRIS) in Salzburg.

angepasstes Grundrecht auf Datenschutz (das entsprechend der Verordnung nunmehr einen Schutz der Daten natürlicher Personen vorsehen sollte), eine Regelung von Datenverarbeitungen zu spezifischen Zwecken sowie auch eine Sonderregelung der Bildverarbeitung.

Während der laufenden Begutachtungsfrist wurde eine Regierungsvorlage in den Nationalrat eingebracht, die dem ursprünglichen Gesetzesentwurf entsprach. Zu dieser Regierungsvorlage wurde – ebenfalls noch innerhalb der Begutachtungsfrist – ein gesamtändernder Abänderungsantrag eingebracht, der nicht nur eine umfangreiche Umstrukturierung und eine Reihe von Änderungen beinhaltete, sondern vor allem auch auf jenen Teil des DSG reduziert war, der keine Regelungen in Verfassungsrang enthielt. Sohin war nicht mehr die Erlassung eines neuen Datenschutzgesetzes, sondern lediglich eine Novelle zum DSG 2000 vorgesehen, wobei die Abkürzung „DSG 2000“ auf „DSG“ umbenannt wurde. Am 29.6.2017 wurde die Novelle im Nationalrat, am 6.7.2017 im Bundesrat beschlossen.

Der Wegfall des verfassungsgesetzlichen Teils führte insbesondere zu Diskussionen, ob das Grundrecht auf Datenschutz auch weiterhin für juristische Personen gelten würde, und zu Irritationen über den Anwendungsbereich des DSG, zumal der Langtitel des novellierten Datenschutzgesetzes sich ausdrücklich nur auf natürliche Personen bezieht.

Am 22.3.2018 wurden zwei Initiativanträge in den Nationalrat eingebracht, wobei ein Antrag, welcher vom Präsidenten des Nationalrates und seiner beiden Stellvertreterinnen unterschrieben wurde,[14] eine DSG-Novelle in Form von zwei Verfassungsbestimmungen enthielt, worin die DSB als unabhängige Aufsichtsbehörde mit der nachprüfenden Kontrolle der Rechtmäßigkeit des Verhaltens des Präsidenten/der Präsidentin des Nationalrates, des Präsidenten/der Präsidentin des Rechnungshofes, des Präsidenten/der Präsidentin des

[14] 188/A.

Verwaltungsgerichtshofes und des/der Vorsitzenden der Volksanwaltschaft als oberste Verwaltungsorgane betraut wurde.

Ein weiterer Antrag, der (ebenfalls) von Abgeordneten der ÖVP, SPÖ und FPÖ eingebracht wurde,[15] enthielt ein Bundesgesetz, mit dem das Bundes-Verfassungsgesetz und das Datenschutzgesetz geändert werden (Datenschutz-Deregulierungs-Gesetz 2018). Die in diesem Initiativantrag vorgesehene Novelle zum DSG enthielt insbesondere wiederum jene Verfassungsbestimmungen, die – aufgrund der im Sommer 2017 fehlenden Zweidrittelmehrheit – nicht beschlossen worden waren. Das Grundrecht auf Datenschutz sollte demgemäß in Hinkunft nur mehr für natürliche Personen gelten. Die in § 2 DSG bisher enthaltene Kompetenzbestimmung sollte aufgrund der Änderung des B-VG entfallen, ebenso § 3, der den räumlichen Geltungsbereich regelt und zu der in der DSGVO enthaltenen Regelung zum räumlichen Anwendungsbereich in einem erheblichen Spannungsverhältnis steht. Weiters enthielt der Initiativantrag einige einfachgesetzliche Änderungen bzw. Ergänzungen des DSG sowie Druckfehlerberichtigungen. Für diese Bestimmungen war – so wie für das ursprüngliche Datenschutz-Anpassungsgesetz – der 25.5.2015 als Termin des Inkrafttretens vorgesehen. Die beiden DSG-Novellen wurden schließlich beschlossen, wobei das Datenschutz-Deregulierungsgesetz jedoch in zweiter Lesung unter Wegfall der Verfassungsbestimmungen stark verändert wurde.[16]

Mehr oder weniger parallel dazu wurden diverse bereichsspezifische Datenschutzregelungen – zusammengefasst zu zwei „Materien-Datenschutz-Anpassungsgesetzen 2018 und einem „Datenschutz-Anpassungsgesetz 2018 - Wissenschaft und Forschung“ – beschlossen.

---

[15] 189/A.
[16] BGBl. I 24/2018.

Die – der grundsätzlich direkten Anwendung der DSGVO geschuldete – „schlanke“ Umsetzung der DSGVO, die sich in erster Linie auf die Öffnungsklauseln stützt, hat zur Folge, dass der Rechtsanwender jene Umsetzungsbestimmungen des ersten, zweiten, vierten und fünften Hauptstückes des DSG stets parallel und ergänzend zur DSGVO lesen muss, da es sich eben lediglich um teilweise Umsetzungen und Ergänzungen handelt. Die Richtlinie 2016/680 wird im 3. Hauptstück des DSG umgesetzt.

4. Eckpunkte der Datenschutz-Grundverordnung

Grundsätzlich ist die DSGVO von der Absicht getragen, die Betroffenenrechte und auch die Datenschutzbehörden zu stärken und einheitliche Kompetenzen vorzusehen, sowie zu gewährleisten, dass der Verantwortliche (auf nach außen sichtbare Art und Weise) der DSGVO und den darin genannten Verpflichtungen des Verantwortlichen entspricht.

4.1. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich gestaltet sich ähnlich wie bei der bisher geltenden Datenschutz-Richtlinie[17]. Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt,
b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

[17] Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, 31.

d) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
e) durch die zuständigen Behörden 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.

Was den räumlichen Anwendungsbereich betrifft, so findet die DSGVO Anwendung

1. auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

2. auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

   a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
   b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

3. auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der der aufgrund des Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

4.2. Rechtmäßigkeit der Datenverarbeitung[18]

Die Grundsätze für die Verarbeitung personenbezogener Daten sind im Großen und Ganzen gleich geblieben und wurden durch das Prinzip der „Rechenschaftspflicht“ ergänzt, das darin besteht, dass der Verantwortliche die DSGVO nicht nur einzuhalten, sondern auch nachzuweisen hat. Prinzipiell besteht daher „mehr sichtbare Verantwortung“ für den für die Datenverarbeitung Verantwortlichen.

Bei den Verarbeitungsvoraussetzungen für nicht-sensible Daten gab es ebenso keine revolutionären Änderungen; allerdings setzt eine Verwendung aufgrund einer Abwägung gemäß Art 6 Abs 1 lit f nunmehr kein „überwiegendes berechtigtes Interesse“ des Verantwortlichen oder eines Dritten voraus, sondern nur ein „berechtigtes Interesse“, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Der Katalog der sensiblen Daten wurde durch genetische und biometrische Daten ergänzt und noch um Ausnahmetatbestände angereichert. Weiters gibt es auch weiterhin eine Bestimmung, die die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten regelt. Auch gibt es eine Bestimmung bezüglich der Bedingungen für die Einwilligung der betroffenen Person und eine weitere, die speziell die Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft regelt.

4.3. Rechte der betroffenen Person[19]

Die Rechte der betroffenen Person bauen auf den herkömmlichen in der Datenschutz-Richtlinie vorgesehenen Rechten auf, werden aber in manchen Details ergänzt. Die notwendigen Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und

[18] Art 5 ff DSGVO.
[19] Art 12 ff DSGVO.

einfachen Sprache zu übermitteln. Neu ist die Frist, innerhalb der die Informationen über die ergriffenen Maßnahmen zu geben sind. Dies hat nämlich bereits innerhalb eines Monats zu erfolgen, die Frist kann aufgrund der Komplexität bzw. bei einer hohen Zahl von Anträgen um maximal weitere zwei Monate verlängert werden. Auch eine Negativauskunft hat innerhalb eines Monats zu erfolgen. Bei offensichtlich unbegründeten oder exzessiven Anträgen kann ein Entgelt verlangt werden oder der Verantwortliche sich weigern, dem Antrag nachzukommen.

Von dem viel diskutierten „Recht auf Vergessenwerden“ ist ein solides Löschungsrecht geblieben, wie es im Wesentlichen bereits auch im DSG 2000 vorgesehen war.

Neu ist das Recht auf Datenübertragbarkeit, wonach die Möglichkeit besteht, die Herausgabe von Datenverarbeitungen, die auf einer Einwilligung der betroffenen Person beruhen und automatisiert vorgenommen werden, vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu verlangen, etwa wenn man einen Providerwechsel anstrebt.

Das Recht auf Einschränkung der Verarbeitung baut im Prinzip auf den Begriff der „Sperre“ von Verarbeitungen auf; nunmehr ist ausdrücklich geregelt, unter welchen Bedingungen eine Datenverarbeitung eingeschränkt werden muss und wofür die Daten dann noch verwendet werden dürfen.

Nach wie vor dürfen Datenverarbeitungen aus bestimmten Gründen auch beschränkt werden: Art 23 Abs 2 DSGVO sieht jedoch vor, dass dies nur durch Gesetze geschehen darf, wenn dies in einer demokratischen Gesellschaft eine notwendige Maßnahme darstellt, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

- Nationale Sicherheit
- Landesverteidigung
- öffentliche Sicherheit
- Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung einschließlich Gefahrenabwehr für die öffentliche Sicherheit
- Schutz eines wichtigen öffentlichen Interesses [insb. wirtschaftliches oder finanzielles Interesse der EU oder eines MS, öffentliche Gesundheit, soziale Sicherheit]
- Schutz der Unabhängigkeit der Justiz
- Verhütung, Ermittlung, Aufdeckung und Verfolgung von Verstößen gegen berufsständische Regeln
- Kontroll-, Überwachungs- und Ordnungsfunktionen, die mit der Ausübung öffentlicher Gewalt verbunden sind
- Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen
- Durchsetzung zivilrechtlicher Ansprüche.

Diese gesetzlichen Einschränkungen haben bestimmten, in Art 23 Abs 2 vorgegebenen Kriterien zu entsprechen.

4.4. Verantwortlicher und Auftragsverarbeiter[20]

4.4.1. Allgemeines

Der Verantwortliche muss geeignete (nach verschiedenen Kriterien abzuwägende!) technische und organisatorische Maßnahmen treffen, um sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung gemäß der DSGVO erfolgt. Diese Pflicht trifft auch den Auftragsverarbeiter.

4.4.2. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

„Datenschutz durch Technikgestaltung“ bedeutet, dass der Verantwortliche geeignete (nach verschiedenen Kriterien

[20] Art 24 ff DSGVO.

abzuwägende!) technische und organisatorische Maßnahmen treffen muss, die insbesondere der Datenminimierung dienen (z. B. Pseudonymisierung).

Datenschutzfreundliche Voreinstellungen bedeuten etwa, dass „by default“ Voreinstellungen, die zur Verarbeitung nur der notwendigsten Daten führen, nicht von vornherein auf „öffentlich“ zu stellen sind, sondern die jeweils datenschutzfreundlichste Voreinstellung zu wählen ist und es der betroffenen Person überlassen bleibt, ob sie die Einstellungen etwa selbst auf „öffentlich“ stellen will.

4.4.3. Auftragsverarbeiter

Weiters sind Regelungen zum Auftragsverarbeiter (bisher nach dem DSG 2000 „Dienstleister“) enthalten. Aufträge, für den Verantwortlichen Daten zu verarbeiten, haben auf Basis vertraglicher Vereinbarungen oder aufgrund eines anderen Rechtsinstruments zu erfolgen. Weiters wird die Vorgangsweise bei der Heranziehung von Sub-Auftragsverarbeitern geregelt. Der Auftragsverarbeiter hat die Daten so zu verarbeiten, dass die Erfüllung der Betroffenenrechte gewährleistet ist; der Verantwortliche hat vom Verantwortlichen die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Auftragsverarbeiters zu erhalten; Auftragsverarbeiter sind an Weisungen des Verantwortlichen gebunden.

4.4.4. Verzeichnis von Verarbeitungstätigkeiten

Die Meldepflicht von Datenverarbeitungen an die Datenschutzbehörde (DSB) entfällt in Hinkunft. Dafür haben der Verantwortliche und der Auftragsverarbeiter Verzeichnisse von Verarbeitungstätigkeiten zu führen (dies gilt nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder schließt sensible oder strafrechtlich relevante Daten ein). Daher ist diese Verpflichtung für jeden Verantwortlichen bzw.

Auftragsverarbeiter, der nicht nur gelegentlich Daten verarbeitet, gegeben.

4.4.5. Datensicherheitsmaßnahmen
Der Verantwortliche und der Auftragsverarbeiter haben Datensicherheitsmaßnahmen einzuhalten, wobei eine Abwägung nach bestimmten in Art 32 DSGVO vorgegebenen Kriterien stattzufinden hat.

4.4.6. Meldung von Datenschutzverletzungen
Vorgesehen ist nunmehr auch eine - gegenüber der bereits im DSG 2000 enthaltenen Bestimmung modifizierte - Meldepflicht von Datenschutzverletzungen (so genannte „data breach notification“). Eine Meldung hat an die Aufsichtsbehörde möglichst binnen 72 Stunden zu erfolgen, es sei denn, es ist voraussichtlich kein Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen gegeben. Weiters sind auch die betroffenen Personen zu informieren, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten besteht. Dies muss nicht erfolgen, wenn geeignete Datensicherheitsmaßnahmen ergriffen wurden, zB durch Verschlüsselung; wenn das hohe Risiko durch Maßnahmen nachträglich beseitigt wurde oder wenn die Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde – in diesem Fall besteht die Verpflichtung einer öffentlichen Bekanntmachung oder Ähnlichem.

4.4.7. Datenschutz-Folgenabschätzung
Eine Datenschutz-Folgenabschätzung ist dann durchzuführen, wenn es sich um voraussichtlich risikoreiche Datenverarbeitungen handelt, wie etwa durch den Einsatz neuer Technologien. Insbesondere sind derartige Folgenabschätzungen bei Profiling, umfangreichen Verarbeitungen sensibler oder strafrechtlich relevanter Daten und einer systematischen Überwachung öffentlich zugänglicher Bereiche geboten. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, bei denen eine Datenschutz-Folgenabschätzung notwendig ist („black list“) und kann auch

eine „white list“ (Verarbeitungsvorgänge, bei denen keine Datenschutz-Folgenabschätzung notwendig ist) erstellen. Die Erstellung einer „white list“ ist im DSG ausdrücklich vorgesehen.

Eine Ausnahme von einer Datenschutz-Folgenabschätzung ist etwa vorgesehen, wenn eine solche bereits vor Erlassung der Rechtsvorschriften, die die Verarbeitungen konkret regeln, stattgefunden hat.

Für den Fall, dass eine Datenschutz-Folgenabschätzung ergibt, dass ein hohes Risiko besteht, ist eine vorherige Konsultation der Aufsichtsbehörde vorgesehen (Art 36). Wenn die geplante Verarbeitung nicht im Einklang zur Verordnung steht, kann die Aufsichtsbehörde (unter Setzung einer Frist) Empfehlungen aussprechen.

4.4.8. Datenschutzbeauftragter

Die Benennung eines Datenschutzbeauftragten (Art 37 ff) ist zwingend bei Behörden oder öffentliche Stellen vorgesehen. Weiters auch im „privaten“ Bereich, wenn die Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und umfangreiche systematische Überwachung der betroffenen Personen erforderlich machen oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten besteht.

Die Benennung eines gemeinsamen Datenschutzbeauftragten für eine Unternehmensgruppe oder mehrere Behörden ist möglich. Fakultativ kann ein Datenschutzbeauftragter auch ohne Vorliegen der zwingenden Voraussetzungen benannt werden, allerdings kommen dann die in der DSGVO vorgesehenen Bestimmungen bezüglich der Rechte und Pflichten des Datenschutzbeauftragten zur Anwendung.
Das DSG sieht in § 5 DSG ergänzende Regelungen zum Datenschutzbeauftragten vor. So ist etwa eine Verschwiegenheitspflicht vorgesehen. Datenschutzbeauftragte im öffentlichen Bereich müssen im Bereich eines

Bundesministeriums diesem oder einer dem Bundesministerium nachgeordneten Dienststelle oder sonstigen Einrichtung angehören. Auch ist unter den Datenschutzbeauftragten des öffentlichen Bereiches ein regelmäßiger Erfahrungsaustausch vorgesehen.

4.5. Übermittlung an Drittstaaten oder an internationale Organisationen[21]

Personenbezogene Daten dürfen dann in Drittstaaten außerhalb der EU übermittelt werden, wenn diese Übermittlung auch innerhalb der EU rechtmäßig wäre und ein Angemessenheitsbeschluss der Kommission (Art 45) bezüglich dieses Drittlandes, dieses Gebietes, oder spezifischer Sektoren eines Drittlands bzw. bezüglich einer internationalen Organisation vorliegt. Derartige Übermittlungen sind genehmigungsfrei. Die vorliegenden Angemessenheitsentscheidungen der Europäischen Kommission bleiben bis auf Weiteres aufrecht. Die Kommission kann auch feststellen, dass kein angemessenes Datenschutzniveau mehr besteht. Diese Beschlüsse werden im Amtsblatt der EU publiziert.

Liegt kein Angemessenheitsbeschluss vor, so kommt eine Datenübermittlung auf der Grundlage geeigneter Garantien (Art 46) in Frage. Demnach können ohne Genehmigung der Aufsichtsbehörde Daten übermittelt werden, wenn rechtlich bindende Instrumente, wie verbindliche interne Vorschriften („Binding Corporate Rules“), Standarddatenschutzklauseln, genehmigte Verhaltensregeln oder genehmigte Zertifizierungsmechanismen vorliegen.

Übermittlungen aufgrund anderer Vertragsklauseln oder Verwaltungsvereinbarungen bedürfen der Genehmigung der Aufsichtsbehörde:

[21] Art 44 ff DSGVO.

Die so genannten „verbindlichen internen Datenschutzvorschriften“ (Art 47) stellen eine rechtliche Selbstbindung in Form von Datenschutzregeln von Unternehmen einer Unternehmensgruppe oder Unternehmen, die in eine gemeinsame Wirtschaftstätigkeit ausüben, dar. Diese werden nunmehr institutionalisiert und näher geregelt.

Weiterhin sind Ausnahmen für Sonderfälle (Art 49) vorgesehen, zB Übermittlungen mit Einwilligung der betroffenen Person; wenn die Übermittlung zur Vertragserfüllung erforderlich ist; wenn wichtige Gründe eines öffentlichen Interesses gegeben sind; wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen stattfindet etc. Weiters wurde eine neue Ausnahme bei nicht wiederholten, nur wenige Personen betreffenden Datenübermittlungen vorgesehen. Die Mitgliedstaaten können im öffentlichen Interesse Vorschriften erlassen, die die Übermittlung bestimmter Datenkategorien ausschließen.

4.6. Datenschutz-Aufsichtsbehörden[22]

Was die Organisation und Bestellung der Aufsichtsbehörden betrifft, so gibt es hier keine wesentlichen Änderungen. Diese sind weiterhin an keine Weisungen gebunden und „völlig unabhängig“. Ihnen sind angemessene personelle, technische und finanzielle Ressourcen, Räumlichkeiten und erforderliche Infrastrukturen zur Verfügung zu stellen. Sie können eigenes Personal aufnehmen und die Finanzkontrolle darf die Unabhängigkeit der Aufsichtsbehörde nicht beeinträchtigen. Sie haben auch eigene, öffentliche Haushaltspläne, die Teil des gesamten Staatshaushalts oder nationalen Haushaltes sein können.

Die Ernennung der Leiter der Aufsichtsbehörden bzw. ihrer Stellvertreter erfolgt durch das Parlament, die Regierung, das Staatsoberhaupt oder eine unabhängige Stelle. Die näheren Modalitäten werden durch Gesetz geregelt. Das DSG hat dazu

[22] Art 51 ff DSGVO.

die bisher geltenden Bestimmungen zur Organisation und zum Bestellmodus übernommen.

Aufgaben der Aufsichtsbehörden sind etwa:

- die Überwachung und Gewährleistung der Anwendung der Verordnung
- die Sensibilisierung der Öffentlichkeit
- Beratung und Aufklärung
- Die Durchführung von Beschwerdeverfahren (wobei der innerstaatliche Gesetzgeber von der Möglichkeit, Verbandsklagen vorzusehen, nicht Gebrauch gemacht hat)
- die Kooperation mit anderen Aufsichtsbehörden
- die Durchführung von Untersuchungen
- die Verfolgung datenschutzrelevanter Entwicklungen
- die Festlegung von Standardvertragsklauseln
- die Erstellung einer Liste der Verarbeitungen, die Datenschutz-Folgenabschätzungen erfordern
- die Abgabe von Stellungnahmen zu den Entwürfen von Verhaltensregeln
- Aufgaben im Zusammenhang mit Zertifizierungsmechanismen
- die Genehmigung von Vertragsklauseln und verbindlichen internen Unternehmensvorschriften
- Beiträge im Europäischen Datenschutzausschuss zu leisten

- interne Aufzeichnungen über Verstöße gegen diese Verordnung und ergriffene Maßnahmen, insbesondere Warnungen und Sanktionen, zu führen
- jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten zu erfüllen.

Darüber hinaus verfügen die Aufsichtsbehörden über Untersuchungsbefugnisse, Abhilfebefugnisse und Genehmigungsbefugnisse und haben jährlich einen Tätigkeitsbericht zu erstellen.

Die Zuständigkeit der Aufsichtsbehörde besteht grundsätzlich im Hoheitsgebiet des Mitgliedstaates. Bei grenzüberschreitenden Datenverarbeitungen ist eine besondere Zuständigkeit der federführenden Aufsichtsbehörde vorgesehen, dabei handelt es sich um die Datenschutzbehörde des Mitgliedstaates, in dem sich die Hauptniederlassung eines Verantwortlichen oder des Auftragsverarbeiters befindet. Die federführende Behörde ist von der Aufsichtsbehörde zu informieren und entscheidet, ob sie die Angelegenheit selbst regelt oder nicht.

4.7. Kohärenz und Europäischer Datenschutzausschuss[23]

Zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden ist eine Zusammenarbeit vorgesehen. Wenn es zu keiner Einigung kommt, greift ein komplexer Zusammenarbeitsmechanismus, das so genannte Kohärenzverfahren. Dies kann auch dazu führen, dass der so genannte Europäische Datenschutzausschuss (siehe dazu gleich) die Entscheidung einer nationalen Aufsichtsbehörde aushebelt und anders entscheidet.

Neu gegründet wird ein Europäischer Datenschutzausschuss, der quasi die Nachfolge der zurzeit bestehenden so genannten

[23] Art 63 ff DSGVO.

„Art 29-Gruppe“ antritt. In diesem Europäischen Datenschutzausschuss sind die Leiter/innen der Aufsichtsbehörden und der Europäische Datenschutzbeauftragte vertreten. Der oder die Vorsitzende wird für fünf Jahre gewählt, das Sekretariat wird vom Europäischen Datenschutzbeauftragten wahrgenommen. Der Europäische Datenschutzausschuss ist unabhängig und hat Rechtspersönlichkeit.

4.8. Rechtsbehelfe, Schadenersatz und Sanktionen[24]

Jede betroffene Person hat das Recht auf Einbringung einer Beschwerde bei der Aufsichtsbehörde. Gegen Entscheidungen der Aufsichtsbehörde kann ein gerichtlicher Rechtsbehelf ergriffen werden. Dies gilt auch für den Fall, dass die Aufsichtsbehörde untätig geblieben ist. Allfällige für den Fall relevante Stellungnahmen oder Beschlüsse des Europäischen Datenschutzausschusses sind dem Gericht zuzuleiten. Zuständig ist jenes Gericht, welches den Sitz im Mitgliedstaat, in dem sich die Aufsichtsbehörde befindet, hat.

Nach Art 79 DSGVO hat jede betroffene Person (unbeschadet der Möglichkeit einer Beschwerde an die Aufsichtsbehörde) das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen den Verantwortlichen oder Auftragsverarbeiter. Das zuständige Gericht ist jenes in dem Mitgliedstaat, in dem der Verantwortliche oder Auftragsverarbeiter seinen Sitz hat oder wo die betroffene Person ansässig ist (außer es handelt sich beim Verantwortlichen um eine Behörde in Ausübung hoheitlicher Befugnisse).

Diese Bestimmung würde eigentlich die Möglichkeit eines parallelen Rechtszuges an die Gerichte bedeuten. Aus den Erläuterungen zum DSG geht hervor, dass bei den Zivilgerichten nur mehr Schadenersatzansprüche geltend gemacht werden können, Datenschutzverstöße jedoch stets bei der Datenschutzbehörde geltend zu machen sind (dahinter

[24] Art 77 ff DSGVO.

steht der Gedanke, dass ansonsten das Recht auf den gesetzlichen Richter verletzt würde bzw. die Problematik der „res iudicata“). Dem steht etwa die Meinung einiger Wissenschafter und Rechtsanwälte entgegen, die die Meinung vertreten, dass Art 79 direkt anwendbar sei.

Die Vertretung von betroffenen Personen kann auch durch eine von diesen beauftragte Einrichtung, Organisation oder einer Vereinigung, die keinen Erwerbszweck verfolgt, erfolgen (die satzungsmäßigen Ziele müssen von öffentlichem Interesse und die Einrichtungen müssen im Datenschutz tätig sein).

4.8.1. Beschwerde an die DSB nach dem DSG (§ 24 DSG)
Im DSG sind nähere verfahrensrechtliche Bestimmungen zum Beschwerdeverfahren bei der DSB vorgesehen. Jede betroffene Person hat das Recht, bei der DSB eine Beschwerde bei einem behaupteten Verstoß gegen die DSGVO oder § 1 oder Art 2, erstes Hauptstück, einzubringen. Die Beschwerde hat bestimmten Kriterien zu genügen und ist binnen eines Jahres ab Kenntnis des beschwerenden Ereignisses, längstens innerhalb von drei Jahren ab dem Ereignis einzubringen. Der Beschwerdegegner kann bis zum Abschluss des Verfahrens bei der DSB die behauptete Rechtsverletzung nachträglich beseitigen. Wenn keine Einwendungen erhoben werden, kommt es zu einer formlosen Einstellung des Verfahrens, ansonsten zur Eröffnung eines neuen Verfahrens (zB wegen „Unvollständigkeit“ einer erteilten Auskunft).

Die betroffene Person ist binnen drei Monaten über den Stand des Verfahrens zu benachrichtigen.

Die DSB kann auch Amtssachverständige heranziehen. Sie kann, wie schon bisher – etwa bei Gefahr im Verzug –, Mandatsbescheide erlassen und Datenverarbeitungen zur Gänze oder teilweise verbieten. Wird die Richtigkeit der Daten bestritten, hat der Beschwerdegegner einen Bestreitungsvermerk anzubringen; allenfalls kann die DSB die

Anbringung eines Bestreitungsvermerks bescheidmäßig anordnen.

Der DSB obliegt auch die Überprüfung der rechtmäßigen Beschränkung einer Datenverarbeitung. Kommt sie zum Schluss, dass die Beschränkung zu Unrecht erfolgte, kann sie z. B. einen Auftrag zur Offenlegung der Daten erteilen.

Die DSB kann auch Genehmigungen von Datenübermittlungen ins Ausland widerrufen, wenn die rechtlichen oder tatsächlichen Voraussetzungen für die Erteilung der Genehmigung nicht mehr bestehen.

4.8.2. Beschwerde an das Bundesverwaltungsgericht

Wie bisher ist es den Parteien möglich, gegen Bescheide der DSB eine Bescheidbeschwerde an das Bundesverwaltungsgericht zu richten. Da die DSB nunmehr viel mehr Kompetenzen als bisher hat, ist davon auch quantitätsmäßig das Bundesverwaltungsgericht betroffen. Bei Untätigkeit der DSB kann wie bisher nach sechs Monaten Säumnisbeschwerde erhoben werden. Weiters kann das Bundesverwaltungsgericht bei einem speziellen Fall der Säumnis angerufen worden, nämlich bei Nicht-Unterrichtung der betroffenen Person über den Stand des Verfahrens innerhalb von drei Monaten durch die DSB. Für diesen Fall hat der Gesetzgeber keine verfahrensrechtliche Vorgangsweise vorgesehen. Man wird daher analog den Bestimmungen zur Säumnisbeschwerde vorgehen müssen, obwohl die Nachholung der Information innerhalb einer viel kürzeren Frist möglich wäre als die Erlassung eines Bescheides, für dessen Nachholung die belangte Behörde drei Monate Zeit hätte.[25]

Nach wie vor sind Senate mit einer Berufsrichterin/einem Berufsrichter und zwei fachkundigen LaienrichterInnen (die auf Vorschlag der WKO und der BAK bestellt werden) vorgesehen. Die LaienrichterInnen müssen mindestens fünf Jahre

[25] S § 16 Bundesgesetz über das Verfahren der Verwaltungsgerichte (Verwaltungsgerichtsverfahrensgesetz – VwGVG), BGBl I 13/2013 idF BGBl. I 138/2017.

einschlägige Berufserfahrung und Kenntnisse des Datenschutzrechtes besitzen.

Bei Bescheiden, denen eine Stellungnahme oder ein Beschluss des Europäischen Datenschutzausschusses vorausgegangen ist, ist diese/r dem BVwG zu übermitteln.

Eine Vertretung der betroffenen Personen durch bestimmte Einrichtungen, Organisationen oder Vereinigungen ist möglich, wobei nunmehr durch das DSG ausdrücklich ausgeschlossen wurde, dass diese Schadenersatz einklagen dürfen.

4.8.3. Schadenersatz

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Der materielle und immaterielle Schadenersatz ist gemäß dem DSG nach den Regelungen des ABGB geltend zu machen. Zuständig ist das für Zivilrechtssachen zuständige Landesgericht, in dessen Sprengel der Kläger seinen gewöhnlichen Aufenthalt hat. Klagen können auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt hat.

4.8.4. Sanktionen

Die Mitgliedstaaten legen Sanktionen für Verstöße, insbesondere für jene, die keiner Verhängung einer Geldbuße

unterliegen, in Rechtsvorschriften fest und ergreifen alle erforderlichen Maßnahmen, um deren Durchführung zu gewährleisten. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Das DSG enthält in § 62 eine entsprechende Verwaltungsstrafbestimmung.

4.9. Geldbußen[26]

Bei der Verhängung von Geldbußen ist eine Reihe von Kriterien zu beachten: die Art, Schwere, und Dauer des Verstoßes; die Frage, ob Vorsätzlichkeit oder Fahrlässigkeit vorliegt; die getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens; der Grad der Verantwortung; allfällige frühere Verstöße; der Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um Abhilfe zu schaffen; die Kategorien personenbezogener Daten; die Art und Weise, wie die Aufsichtsbehörde vom Verstoß Kenntnis bekommen hat; die Einhaltung bereits angeordneter Maßnahmen und andere erschwerende oder mildernde Umstände.

Bei bestimmten Delikten beträgt die Höhe maximal EUR 10.000.000 oder im Falle eines Unternehmens bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (zB bei Verletzung bestimmter den Verantwortlichen treffenden Verpflichtungen).

Bei gröberen Verstößen können Geldbußen von bis zu EUR 20.000.000 oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden (zB bei Verstößen gegen die Datenverarbeitungsgrundsätze, bei Verstößen gegen die Rechte der betroffenen Personen, bei Verstößen bei der Übermittlung in Drittstaaten, bei Nichtbefolgung von Anweisungen der Aufsichtsbehörde).

[26] Art 83 DSGVO.

Die Mitgliedstaaten können vorsehen, ob und welche Geldbußen gegen Behörden und öffentliche Stellen verhängt werden können. Sieht die Rechtsordnung eines Mitgliedstaates keine Geldbußen vor, kann die Aufsichtsbehörde die Geldbuße in die Wege leiten und die Geldbuße von den nationalen Gerichten verhängt werden.[27]

Im DSG werden allgemeine Bedingungen für die Verhängung von Geldbußen festgelegt: Eine Verhängung von Geldbußen gegen eine juristische Person ist möglich, wenn Verstöße (gegen DSGVO oder § 1 oder Art 2 erstes Hauptstück des DSG) durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben oder eine Führungsposition innerhalb der juristischen Person innehaben. Auch bei mangelnder Überwachung der Kontrolle dieser Personen kann eine Geldbuße verhängt werden. Von einer Verwaltungsstrafe gegenüber einem Verantwortlichen nach § 9 VStG ist abzusehen, wenn für denselben Verstoß bereits eine Strafe gegen die juristische Person verhängt wurde.

Rechtskräftige Bescheide der DSB sind Exekutionstitel, die Bewilligung ist bei dem Bezirksgericht, in dessen Sprengel der Verpflichtete seinen allgemeinen Gerichtsstand in Streitsachen hat, zu beantragen. Gegen Behörden, öffentliche Stellen und Körperschaften öffentlichen Rechts können keine Geldbußen verhängt werden.

4.10. Vorschriften für besondere Datenverarbeitungssituationen

Kapitel IX DSGVO enthält Regelungen für besondere Datenverarbeitungssituationen, die durch die Mitgliedstaaten näher ausgeführt werden können. Es sind dies:

[27] Diese Bestimmung betrifft laut ErwGr 151 Dänemark und Estland.

- Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
- Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten
- Verarbeitung einer nationalen Kennziffer
- Datenverarbeitung im Beschäftigungskontext
- Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken und zu statistischen Zwecken
- Geheimhaltungspflichten
- Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

5. Zusammenfassung

Die DSGVO baut auf der Richtlinie 95/46/EG auf und ist daher wohl eher als „Evolution“ statt als „Revolution“ aufzufassen. Die Problematik der DSGVO ergibt sich allerdings aus einer Anzahl von interpretationsbedürftigen Bestimmungen, deren Auslegung der DSB und in weiterer Folge den Gerichten obliegen wird. Letztendlich ist eine Reihe von Vorlagen an den EuGH zu erwarten.

Als positiv ist die „schlanke“ Durchführung/Umsetzung im DSG zu sehen, wenngleich sich dadurch eine schwerere Lesbarkeit ergibt, weil DSGVO und DSG immer parallel gelesen werden müssen. Andererseits wurden bereits beim Datenschutz-Anpassungsgesetz 2018 bedeutsame Anregungen nicht mehr berücksichtigt, die auch keinen Eingang in die beiden Initiativanträge gefunden haben, die letztendlich (z.T. stark verändert) als Novellen zum DSG beschlossen wurden. Besonders bedauerlich und sachlich nicht nachvollziehbar ist das neuerliche Scheitern einer Novellierung der Verfassungsbestimmungen der §§ 1 bis 3 DSG. Damit ist nicht nur eine Kompetenzbereinigung wiederum gescheitert, sondern

wirft auch die Weitergeltung des Grundrechts für juristische Personen eine Reihe von rechtlichen Fragen auf.

Bemerkenswert ist es, dass es bei den Neuregelungen sogar teilweise zu Unterschreitungen des bisherigen österreichischen Datenschutzniveaus kommt.

Last not least ist festzustellen, dass es sich auch jetzt noch lohnt, sich mit der neuen Rechtslage auseinanderzusetzen, zumal davon auszugehen ist, dass sie uns noch einige Jahre begleiten wird.

Die Umsetzung der RL 2016/680 und deren Auswirkungen auf das Straf- und Strafprozessrecht

Dr. Roland Pichler
Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, vormals Universität Wien

1. Einleitung

Die Richtlinie (EU) 2016/680[28] (auch JI-Richtlinie)[29] bildet gemeinsam mit der Datenschutzgrundverordnung (DSGVO)[30] den Datenschutzrahmen der Europäischen Union. Beide Gesetzgebungswerke wurden am 27. April 2016 erlassen. Während die DSGVO am 24. Mai 2016 in Kraft trat (Art 99 Abs 1 DSGVO), aber erst seit dem 25. Mai 2018 anzuwenden ist (Art 99 Abs 2 DSGVO), lief die Umsetzungsfrist der JI-Richtlinie bis zum 6. Mai 2018 (Art 63 Abs 1 JI-Richtlinie).

Weder die DSGVO noch die JI-Richtlinie haben unmittelbaren Einfluss auf das materielle Strafrecht. Diverse Begriffe des Computerstrafrechts waren zwar nach den Definitionen des DSG 2000 auszulegen, wie etwa der Begriff der personenbezogenen Daten in § 118a StGB. Die nunmehr dafür heranzuziehenden Definitionen der DSGVO bringen aber für diesen Bereich keine inhaltlichen Änderungen mit sich. Das Delikt des bisherigen § 51 DSG 2000, nämlich die

[28] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 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.
[29] Justiz und Inneres.
[30] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Datenverwendung in Gewinn- oder Schädigungsabsicht, findet sich nun inhaltlich unverändert in § 63 DSG 2018[31] und trägt nunmehr im Titel den Begriff Datenverarbeitung statt Datenverwendung.
Die JI-Richtlinie umfasst 64 Artikel und 107 Erwägungsgründe. Die innerstaatliche Umsetzung erfolgte in Österreich im 3. Hauptstück (§§ 36–61) des DSG 2018. Aufgrund des Umfangs der Richtlinie bzw. der Umsetzungsbestimmungen, können im Folgenden nur wesentliche Eckpunkte dargestellt werden.

2. Regelungsgegenstand und Anwendungsbereich

2.1. Anwendungsbereich

Die JI-Richtlinie regelt die Verarbeitung[32] personenbezogener Daten[33] durch die zuständigen Behörden[34] zu den in Art 1 Abs 1 JI-Richtlinie genannten Zwecken[35] (Art 2 Abs 1 JI-Richtlinie). Damit der Anwendungsbereich eröffnet ist, muss die Verarbeitung ganz oder teilweise automatisiert erfolgen. Bei personenbezogenen Daten die nichtautomatisiert verarbeitet werden, ist die Richtlinie nur dann anzuwenden, wenn diese „manuellen" Daten in einem Dateisystem[36] gespeichert sind oder gespeichert werden sollen (Art 2 Abs 2 JI-Richtlinie). Von einem Dateisystem wird dann gesprochen, wenn zB bei einem Aktensystem durch die vorgegebene Ordnung ein systematischer Zugriff auf Personendaten möglich ist.[37]

Jedenfalls keine Anwendung findet die Richtlinie auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des

---

[31] Der Kurztitel des „Datenschutzgesetz 2000 – DSG 2000" wurde mit BGBl I Nr. 120/2017 auf „Datenschutzgesetz – DSG" geändert. Zur besseren Unterscheidung wird für letzteres in diesem Beitrag die Bezeichnung „DSG 2018) verwendet.
[32] Zur Definition der Verarbeitung siehe Art 3 Z 2 JI-RL.
[33] Zur Definition von personenbezogenen Daten siehe Art 3 Z 1 JI-RL.
[34] Siehe dazu Kapitel 2.3.
[35] Siehe dazu Kapitel 2.2.
[36] Die englische Übersetzung der JI-RL spricht treffender von „filing system".
[37] Die DSGVO hat bezüglich der Verarbeitung den gleichen sachlichen Anwendungsbereich (Art 2 Abs 1 DSGVO). Zu den Begrifflichkeiten siehe etwa Auernhammer/*von Lewinski* Art 2 Rn 6ff.

Unionsrechts fällt (Art 2 Abs 3 lit a JI-Richtlinie) sowie auf die die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union (Art 2 Abs 3 lit b JI-Richtlinie).

2.2. Ziel und Zweck der JI-Richtlinie

Die Verhütung, Aufdeckung und Verfolgung von Straftaten ist vom Anwendungsbereich der DSGVO ausgenommen (Art 2 Abs 2 lit d DSGVO), da für diesen Bereich strengere und speziellere Vorschriften, sowie ein größerer mitgliedsstaatlicher Gestaltungsspielraum notwendig sind.[38] Als ergänzendes Regelungswerk wurde daher die JI-Richtlinie erlassen, welche den 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 zum Gegenstand hat (Art 1 Abs 1 JI-Richtlinie).

Die JI-Richtlinie hat das Ziel, im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit ein einheitliches und hohes Schutzniveau für die personenbezogenen Daten natürlicher Personen zu gewährleisten bzw. den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedsstaaten zu erleichtern (EG 7 der JI-Richtlinie). Die JI-Richtlinie umfasst daher die Bereiche der Sicherheitspolizei, des polizeilichen Staatsschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzuges. In Österreich wurden die Umsetzungsbestimmungen noch auf die Bereiche der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung ausgeweitet (§ 36 Abs 1 DSG 2018). Durch diese Ausweitung werden also auch Datenverarbeitungen erfasst, die nicht in den Anwendungsbereich des Unionsrechts fallen.[39]

---

[38] Auernhammer/*von Lewinski* Art 2 Rn 35.

[39] Dazu auch Bergauer, Gesetzgebungsmonitor Datenschutz: Umsetzungsentwurf der Datenschutz-Richtlinie-Strafrecht (EU) 2016/680, jusIT 2017, 158.

2.3. Zuständige Behörde

Adressat der JI-Richtlinie bzw. der Umsetzungsbestimmungen ist die zuständige Behörde. Eine zuständige Behörde iSd § 36 Abs 1 DSG 2018 ist entweder „eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, die nationale Sicherheit, den Nachrichtendienst oder die militärische Eigensicherung zuständig ist“ (§ 36 Abs 2 Z 7 lit a DSG 2018), oder „eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zum Zweck der nationalen Sicherheit, des Nachrichtendienstes oder der militärischen Eigensicherung übertragen wurde“ (§ 36 Abs 2 Z 7 lit b DSG 2018).[40]

Sowohl die Richtlinie als auch die Umsetzungsbestimmungen verfolgen einen funktionalen und keinen organisatorischen Ansatz.[41] Die zuständigen Behörden haben also die Vorschriften des 3. Hauptstücks des DSG 2018 nur dann anzuwenden, wenn die konkrete Datenverarbeitung den in § 36 Abs 1 DSG 2018 genannten Zwecken dient. Wird zB die Polizei zu anderen Zwecken tätig, denken wir etwa an Versammlungen, gelten für Datenverarbeitungen in diesem Zusammenhang die Bestimmungen der DSGVO. Bei Grenzfällen, bei denen auf den ersten Blick unklar ist, ob die Datenverarbeitung in einem Zusammenhang mit einem in § 36 Abs 1 DSG 2018 genannten Zweck steht, sind bis zur Klärung des Zuständigkeitsbereiches die Regelungen des 3. Hauptstücks des DSG 2018 anzuwenden. Beispiele für

[40] Ursprünglich wurden die Bereiche der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung bei der Definition der zuständigen Behörde „vergessen“ (BGBl I 120/2017). Mit BGBl. I 24/2018 wurde, neben anderen Änderungen und Anpassungen, dieses Versehen ausgebessert.

[41] ErlRV 1664 BlgNR XXV. GP, 17.

solche Grenzfälle sind etwa ein Unfall oder Suizid. Solange hier eine Straftat nicht ausgeschlossen werden kann, ist nach den Bestimmungen des 3. Hauptstücks des DSG 2018 vorzugehen.[42]

3. Grundsätze der Datenverarbeitung

Die Grundsätze der Verarbeitung von personenbezogenen Daten sind in § 37 Abs 1 DSG 2018 bzw. Art 4 JI-Richtlinie geregelt. Die Verarbeitung muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben erfolgen. Die Daten dürfen dabei nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Rechtmäßig ist die Verarbeitung personenbezogener Daten dann, wenn sie zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, oder wenn sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen ist und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs 1 DSG 2018 genannten Zwecken wahrgenommen wird (§ 38 DSG 2018).

Die personenbezogenen Daten müssen dem Verarbeitungszweck entsprechen, maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein. Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sind unverzüglich zu löschen bzw. zu berichtigen. Sie dürfen nicht länger, als es für den Zweck, für den sie verarbeiten werden, erforderlich ist, in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person möglich macht. Daraus folgt auch, dass Daten die unrichtig, unvollständig, nicht mehr aktuell oder zu löschen sind, auch nicht übermittelt oder einer automatisierten Verarbeitung unterzogen werden dürfen (§ 37 Abs 6 DSG 2018).

[42] ErlRV 1664 BlgNR XXV. GP, 16; EG 12 der JI-Richtlinie.

Personenbezogene Daten können dabei auch für einen anderen Zweck, als den für den sie erhoben werden, verarbeitet werden, sofern dieser Zweck vom Anwendungsbereich des § 36 Abs 1 DSG 2018 umfasst ist, durch Rechtsvorschriften geregelt und die Verarbeitung für den anderen Zweck erforderlich und verhältnismäßig ist[43] (§ 40 Abs 1 DSG 2018, EG 29 der JI-Richtlinie). Sollen die Daten für andere, nicht von § 36 Abs 1 DSG 2018 umfasste Zwecke, weitergegeben werden, so muss auch dies gesetzlich vorgesehen sein und der Empfänger zur Verarbeitung für den anderen Zweck befugt sein (§ 40 Abs 2 DSG 2018).

Geheime Ermittlungsmaßnahmen stehen diesen Grundsätzen zwar nicht entgegen, sofern sie durch Rechtsvorschriften geregelt und in einer demokratischen Gesellschaft erforderlich und verhältnismäßig sind. Dabei sind die Interessen der betroffenen Person gebührend zu berücksichtigen (EG 26 der JI-Richtlinie). Die dargelegten Grundsätze werden aber bei geheimen Ermittlungsmaßnahmen zusätzlich zu grundrechtlichen Aspekten zu berücksichtigen sein. Dies wird vor allem für die ab 1. April 2020 mögliche „Überwachung verschlüsselter Nachrichten“[44] (§ 135a StPO de lege ferenda) von Relevanz sein, bei der Ermittlungsbehörden, je nach technischer Ausgestaltung, eine Fülle von personenbezogenen Daten sozusagen als Beifang abgreifen, die für den Ermittlungszweck nicht relevant sind. Ähnliches gilt auch für Funkzellenabfragen und in eingeschränktem Maße für Telefonüberwachungen.

Für die Verarbeitung von besonderen Kategorien personenbezogener Daten gelten dabei gehobene Anforderungen (§ 39 DSG 2018, Art 10 JI-Richtlinie). Die besonderen Kategorien personenbezogener Daten wurden nach dem bisherigen österreichischen Datenschutzrecht als sensible oder besonders schutzwürdige Daten bezeichnet (§ 4

[43] Also die Voraussetzungen der §§ 38, 39 DSG 2018 erfüllt sind.
[44] Auch unter den Schlagworten „Online-Durchsuchung“, „Bundestrojaner“ bzw. Staatstrojaner bekannt.

Z 2 DSG 2000). Das sind also Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Weiters gehören dazu auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Die Verarbeitung solcher Daten ist nur zulässig, wenn sie unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden. Zusätzlich muss mindestens einer der drei folgenden Tatbestände vorliegen: Die Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig, oder die Verarbeitung dient der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person, oder die Verarbeitung betrifft Daten, die die betroffene Person offensichtlich öffentlich gemacht hat.[45]

Diese Bestimmungen haben Auswirkungen auf geheime Ermittlungsmaßnahmen, wie etwa die Telekommunikationsüberwachung oder die geplante Online-Durchsuchung. Bei diesen Ermittlungsmaßnahmen ist die Gefahr sehr hoch, dass besondere Kategorien personenbezogener Daten verarbeitet werden. Dabei stellt sich die Frage, wie hier die Schutzmöglichkeiten der betroffenen Personen auszugestalten sind. Eine Möglichkeit wäre etwa, die Überwachungsdaten durch eine unabhängige Stelle vorab auswerten zu lassen,[46] und die Löschung der besonderen Kategorien von personenbezogenen Daten zu veranlassen, die für das weitere Verfahren nicht relevant sind.

---

[45] „Öffentlich sind Daten, wenn eine unbegrenzte Anzahl von Personen ohne Zugriffsbeschränkung (Passwort, Berechtigung, etc.) auf diese zugreifen kann." (Auernhammer/*Greve* Art 9 Rn 25).

[46] Etwa durch den Rechtsschutzbeauftragten, der dann aber personell aufgestockt werden müsste.

4. Pflichten des Verantwortlichen

Kapitel IV der JI-Richtlinie enthält die Pflichten des Verantwortlichen (§§ 46, 54 DSG 2018),[47] also der für die jeweilige Datenverarbeitung konkret zuständige Stelle.[48] Der Verantwortliche hat geeignete technische[49] und organisatorische Maßnahmen zu treffen. Damit sollen Datenschutzgrundsätze, wie etwa Datenminimierung, und die Anforderungen der JI-Richtlinie wirksam umgesetzt werden, also auch der Schutz der Rechte betroffener Personen sichergestellt werden (Art 20 Abs 1 JI-Richtlinie). So sieht § 50 DSG 2018 vor, dass jeder Verarbeitungsvorgang zu protokollieren ist, damit die Zulässigkeit des Zugriffs nachvollzogen werden kann (Art 25 JI-Richtlinie). Durch Voreinstellungen in der jeweiligen Datenverarbeitung soll sichergestellt werden, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für einen bestimmten Verarbeitungszweck erforderlich ist. Das betrifft die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit der Daten (Art 20 Abs 2 JI-Richtlinie).[50] Diese Vorgaben werden bei den geheimen technischen Ermittlungsmaßnahmen[51] zu berücksichtigen sein.

Ebenso wie bei der DSGVO ist vorgesehen, dass ein Verzeichnis der Verarbeitungstätigkeiten geführt wird (§ 49 DSG 2018, Art 24 JI-Richtlinie) und in bestimmten Fällen eine Datenschutz-Folgenabschätzung durchzuführen ist (§ 52 DSG 2018, Art 27 JI-Richtlinie). Ist die Verarbeitung personenbezogener Daten durch neue Systeme bzw. Technologien geplant, so kann dies unter bestimmten

---

[47] Auf die Pflichten des Auftragsverarbeiters, welche auch in Kapitel IV geregelt sind, soll hier aus Platzgründen nicht näher eingegangen werden. Zum Auftragsverarbeiter siehe Art 22 JI-Richtlinie.

[48] Bei mehreren Verantwortlichen liegt eine „gemeinsame Verantwortlichkeit“ vor, siehe Art 21 JI-RL.

[49] § 54 DSG 2018 enthält einen Katalog an Datensicherheitsmaßnahmen.

[50] Diese Maßnahmen können unter die Schlagworte „privacy by design“ und „privacy by default“ subsumiert werden. Siehe dazu auch Art 25, 32 DSGVO und die dazu erfolgten Kommentierungen wie etwa Auernhammer/*Brügemann* Art 24; Auernhammer/*Kramer/Meints* Art 32.

[51] ZB Funkzellenabfrage, Überwachung verschlüsselter Nachrichten, Telefonüberwachung.

Umständen die Konsultation der Aufsichtsbehörde notwendig machen (§ 53 DSG 2018, Art 28 JI-Richtlinie).

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten[52], ist die Aufsichtsbehörde unverzüglich ab Bekanntwerden, möglichst jedoch binnen 72 Stunden zu unterrichten.[53] Einer späteren Meldung ist eine Begründung für die Verzögerung hinzuzufügen. Keine Meldung ist vorzunehmen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (§ 55 DSG 2018, Art 30 Abs 1 JI-Richtlinie).[54] Neben der Aufsichtsbehörde ist die betroffene Person dann zu informieren, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (§ 56 DSG 2018, Art 31 JI-Richtlinie). Im Vergleich zu Art 30 JI-Richtlinie besteht hier ein umgekehrtes Regel-Ausnahme-Prinzip, welches die Schwelle für eine Benachrichtigungspflicht anhebt.[55]

Der Verantwortliche, also die jeweils zuständige Behörde, hat einen Datenschutzbeauftragten zu benennen. Gerichte sind im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen (§ 57 DSG 2018).[56] Ein Datenschutzbeauftragter kann auch für mehrere zuständige Behörden bestellt werden, wobei Größe und Organisationsstruktur der Behörden zu berücksichtigen sind (Art 32 Abs 3 JI-Richtlinie). Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Datenschutzbehörde mitzuteilen (§ 57 Abs 4 DSG 2018, Art 32 Abs 4 JI-Richtlinie). Der Datenschutzbeauftragte ist rechtzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängender Fragen einzubinden (Art 33 JI-Richtlinie).

---

[52] Zur Definition siehe Art 3 Z 11 JI-Richtlinie. Auch Auernhammer/*Schreibauer* Art 33 Rn 5f.
[53] Zum Inhalt der Meldung siehe Art 30 Abs JI-Richtlinie.
[54] Dazu etwa Auernhammer/*Schreibauer* Art 33 Rn 10f; Artikel-29-Datenschutzgruppe, „Guidelines on Personal data breach notification under Regulation 2016/679“, WP 250.
[55] Zur identen Regelung in der DSGVO siehe etwa Auernhammer/*Schreibauer* Art 33 Rn 10f, Art 34 Rn 3ff.
[56] Der österreichische Gesetzgeber hat von dieser Kann-Bestimmung in Art 32 JI-Richtlinie Gebrauch gemacht.

Dem Datenschutzbeauftragten obliegt die Unterrichtung und Beratung der Verantwortlichen und Beschäftigten hinsichtlich datenschutzrechtlicher Fragestellungen, die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften, die Beratung bei Datenschutz-Folgenabschätzungen sowie die Zusammenarbeit mit der Aufsichtsbehörde (§ 57 Abs 3 DSG 2018,[57] Art 34 JI-Richtlinie).

5. Rechte der betroffenen Personen

Damit die betroffenen Personen in die Lage versetzt werden ihre Rechte wahrzunehmen, müssen sie über ein Mindestmaß an Informationen verfügen. Diese Informationen sind vom Verantwortlichen bereitzustellen und beinhalten etwa die Zwecke der Datenverarbeitung.[58] Von der Informationspflicht bestehen allerdings Ausnahmen, die vor allem bei geheimen Ermittlungsmaßnahmen zur Anwendung kommen werden. Die Unterrichtung der betroffenen Person kann soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden, sofern ein solches Vorgehen in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und soweit den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird. Eine solche Informationseinschränkung ist zulässig (§ 43 Abs 4 DSG 2018, Art 13 Abs 3 JI-Richtlinie):

- zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,
- zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,
- zum Schutz der öffentlichen Sicherheit,
- zum Schutz der nationalen Sicherheit,
- zum Schutz der Rechte und Freiheiten anderer.

[57] Mit Verweis auf Art 39 DSGVO.
[58] Zu den Modalitäten und Inhalt der Informationsverteilung siehe die Art 12, 13 JI-Richtlinie.

Die betroffenen Personen haben ein Auskunftsrecht, ob personenbezogene Daten verarbeitet werden und wenn ja, zu welchem Zweck und aufgrund welcher Rechtsgrundlage, welche Kategorien von personenbezogenen Daten, mit wem die Daten ausgetauscht worden sind, die geplante Speicherdauer (§ 44 DSG 2018, Art 14 JI-Richtlinie). Ähnlich der Informationspflicht, kann auch das Auskunftsrecht unter den gleichen Voraussetzungen eingeschränkt werden (§ 44 Abs 2 DSG 2018, Art 15 Abs 1 JI-Richtlinie). Die betroffene Person ist über die Verweigerung oder Einschränkung des Auskunftsrechtes zu informieren, sofern die Verständigung nicht wieder jenen Zwecken zuwiderliefe, wegen denen das Auskunftsrecht versagt oder eingeschränkt wurde (§ 44 Abs 3 DSG 2018, Art 15 Abs 3 JI-Richtlinie). Kommt es zu einer Verweigerung oder Einschränkung des Auskunftsbegehrens, ist dies zu dokumentieren (§ 44 Abs 4 DSG 2018, Art 15 Abs 4 JI-Richtlinie).

Die Auskunft bzw. die in diesem Zusammenhang getroffenen Maßnahmen müssen innerhalb eines Monats nach Eingang des Antrages erteilt werden. Die Frist kann um zwei Monate verlängert werden, falls dies die Komplexität und die Anzahl der Anträge erforderlich macht (§ 42 Abs 4 DSG 2018).

Bei exzessiven oder offenkundig unbegründeten Anträgen kann ein angemessenes Entgelt verlangt oder die Auskunftserteilung verweigert werden (§ 42 Abs 6 DSG 2018, Art 12 Abs 4 JI-Richtlinie).

Die betroffenen Personen haben das Recht auf Berichtigung oder Löschung der personenbezogenen Daten bzw. auf Einschränkung der Verarbeitung. Die Daten sind vom Verantwortlichen oder auf Antrag der betroffenen Personen unverzüglich zu löschen, wenn sie für die Zwecke für die sie erhoben worden sind, nicht mehr notwendig sind, wenn sie unrechtmäßig verarbeitet wurden bzw. wenn die Löschung zur Erfüllung einer rechtlichen Verpflichtung notwendig ist (§ 45 DSG 2018, Art 16 JI-Richtlinie). Diese Rechte können unter den

in § 45 Abs 3 DSG 2018 genannten Voraussetzungen eingeschränkt werden. Wie sich diese Rechte und deren Einschränkung auf das Strafverfahren auswirken, zB bezüglich des Themas Beweisverwertungsverbot, müsste noch näher untersucht werden.

Werden die Informations-, Auskunfts-, Lösch- oder Berichtigungsrechte der Person eingeschränkt oder verweigert, kann die Aufsichtsbehörde angerufen werden (§ 42 Abs 8, 9 DSG 2018, Art 17 JI-Richtlinie).

6. Rechtsbehelfe

Betroffene Personen haben das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die nach der JI-Richtlinie erlassenen Vorschriften verstößt (Art 52 JI-Richtlinie). Gegen die Entscheidung der Aufsichtsbehörde muss ein wirksamer gerichtlicher Rechtsbehelf (Art 53 JI-Richtlinie) bestehen. In Österreich wurde die Datenschutzbehörde als Aufsichtsbehörde festgelegt (§ 32 DSG 2018), wobei gegen Entscheidungen der Datenschutzbehörde der Gang zum Bundesverwaltungsgericht offensteht (§ 27 DSG 2018).

Art 54 JI-Richtlinie verlangt einen wirksamen gerichtlichen Rechtsbehelf, der gegen die Verantwortlichen oder Auftragsverarbeiter gerichtet ist, und zwar unabhängig eines außergerichtlichen oder verwaltungsrechtlichen Rechtsbehelfs, oder des Rechts der Beschwerde bei einer Aufsichtsbehörde. Dieser Rechtsweg soll dann beschritten werden können, wenn die betroffene Person der Meinung ist, dass Rechte, die ihr aufgrund der nach der JI-Richtlinie erlassenen Vorschriften zustehen, verletzt wurden, weil die Verarbeitung ihrer personenbezogenen Daten nicht im Einklang mit diesen Vorschriften stand. Diese Regelung wurde in Österreich nicht umgesetzt. Auch ist fraglich, welchen Zweck die Regelung

verfolgt, wenn ohnehin ein Beschwerderecht an die Aufsichtsbehörde samt Rechtsmittel zur Verfügung steht.[59]

Die in Art 52–54 JI-Richtlinie genannten Rechte können auch von einer gemeinnützigen Organisation wahrgenommen werden, deren satzungsgemäße Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind (§ 29 DSG 2018, Art 55 JI-Richtlinie).

Eine Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen Handlung, die gegen nach Maßgabe dieser Richtlinie erlassenen nationalen Vorschriften verstößt, ein materieller oder immaterieller Schaden entstanden ist, hat das Recht auf Schadenersatz seitens des Verantwortlichen oder jeder sonst nach dem Recht der Mitgliedstaaten zuständigen Stelle (Art 56 JI-Richtlinie). Diese Bestimmung wurde in Österreich nicht umgesetzt. Fraglich ist, ob es dafür einer eigenen Bestimmung bedarf,[60] oder nicht ohnehin der zivilrechtliche Weg offensteht.

7. Aufsichtsbehörde

Zur Überwachung der Anwendung der Richtlinie sind von den Mitgliedstaaten eine oder mehrere unabhängige Behörden einzurichten (Aufsichtsbehörden). Damit sollen die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt und der freie Verkehr personenbezogener Daten in der Union erleichtert werden (Art 41 Abs 1 JI-Richtlinie). Zu diesem Zweck haben die Aufsichtsbehörden sowohl untereinander als auch mit der Kommission zusammenzuarbeiten (Art 41 Abs 2 JI-Richtlinie).[61] Die für die Überwachung der Anwendung der DSGVO zuständige Aufsichtsbehörde (Art 51 DSGVO), kann auch als Aufsichtsbehörde gem. Art 41 JI-Richtlinie fungieren (Art 41

[59] Siehe auch unten die Ausführungen zu Art 56 JI-Richtlinie (Schadenersatz).
[60] Siehe für den Bereich der DSGVO § 29 DSG 2018.
[61] Detaillierte Mechanismen zur Zusammenarbeit sind in Kapitel VII JI-Richtlinie geregelt.

Abs 3 JI-Richtlinie). Von dieser Möglichkeit wurde in Österreich Gebrauch gemacht und die Datenschutzbehörde als Aufsichtsbehörde festgelegt (§ 31 DSG 2018). Wobei die Datenschutzbehörde nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist.

Die Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse völlig unabhängig. Sie muss mit entsprechenden personellen,[62] technischen, finanziellen und infrastrukturellen Ressourcen ausgestattet sein, um ihre Aufgaben effektiv wahrnehmen zu können (Art 42 JI-Richtlinie). Dadurch soll einer zahnlosen Behörde entgegengewirkt werden, die zwar formal existiert, ihre Aufgaben jedoch aufgrund mangelnder Mittel nicht in erforderlichem Ausmaß wahrnehmen könnte.

Die Aufsichtsbehörde verfügt über wirksame Untersuchungsbefugnisse, wie etwa den Zugang zu allen personenbezogenen Daten und allen weiteren Informationen, die zur Aufgabenerfüllung notwendig sind. Die Aufsichtsbehörde kann einen Verantwortlichen warnen, wenn beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die Richtlinie bzw. deren Umsetzungsvorschriften verstoßen. Sie kann ihn anweisen, Verarbeitungsvorgänge in Einklang mit der Richtlinie zu bringen (§ 33 DSG 2018). Die Datenschutzbehörde kann aber auch überhaupt eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich des Verbots, verhängen.

Als weiteres Instrument der Kontrolle dient Art 48 JI-Richtlinie (§ 34 Abs 1 und 2 DSG 2018). Demnach haben die Mitgliedstaaten vorzusehen, dass die zuständigen Behörden wirksame Vorkehrungen treffen, um vertrauliche Meldungen über Verstöße gegen diese Richtlinie zu fördern („Whistleblowing“).

[62] Zu den Anforderungen an die Mitglieder der Aufsichtsbehörden siehe Art 43 JI-Richtlinie.

8. Internationaler Datenaustausch

Die Übermittlung von personenbezogenen Daten an Drittländer oder internationale Organisationen ist im 4. Abschnitt des 3. Hauptstückes DSG 2018 geregelt.[63] Eine solche Übermittlung ist nur zulässig, wenn sie für die in § 36 Abs 1 DSG 2018 genannten Zwecke erforderlich ist und an eine für solche Zwecke zuständige Behörde erfolgt. Für den Drittstaat oder die Internationale Organisation muss zudem entweder

- ein Angemessenheitsbeschluss der Kommission vorliegen. Vereinfacht gesagt bedeutet das, dass die Kommission der Meinung ist, dass der Drittstaat oder die Internationale Organisation ein entsprechendes Schutzniveau aufweist (Art 36 JI-Richtlinie)
- oder, es müssen geeignete Garantien für den Schutz von personenbezogenen Daten im Drittland oder bei der internationalen Organisation vorliegen (Art 37 JI-Richtlinie)

Gibt es weder einen Angemessenheitsbeschluss und liegen auch keine geeigneten Garantien vor, dann ist die Übermittlung in bestimmten Ausnahmefällen zulässig, etwa wenn der Datenaustausch zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaates oder eines Drittlandes dient. (§ 59 Abs 6 u 7 DSG 2018, Art 38 JI-RL).

9. Fazit

Mit dem Anwendungsbeginn der DSGVO hat sich bei Unternehmen und Organisationen, sei es nun im öffentlichen oder nichtöffentlichen Bereich, mitunter eine Panikstimmung verbreitet. Die Gründe hierfür sind vielfältig: Es wurde mit der Umsetzung der neuen Regelungen zu lange zugewartet, der Informationsstand war schlecht und hinzu kamen die abschreckend hohen Maximalgeldbußen der DSGVO.

[63] In der JI-RL in Kapitel V.

Im Gegensatz dazu drangen Stimmungsbilder der von der JI-Richtlinie betroffenen Behörden nicht nach außen. Wie gut die zuständigen Behörden auf die praktische Anwendung der durch die JI-Richtlinie gemachten Vorgaben vorbereitet sind, wird sich daher erst zeigen. Denn die Umsetzung der JI-Richtlinie ist nur der erste Schritt, welchem die konsequente Anwendung der Bestimmungen in der täglichen Praxis folgen sollte. Etliche Probleme, die zunächst nicht bedacht wurden, werden erst im Laufe der Zeit zum Vorschein kommen, wie dies auch derzeit im Anwendungsbereich der DSGVO zu beobachten ist. Ein wichtiger Aspekt wird dabei auch sein, wie die Datenschutzbehörde ihre Aufgabe gegenüber den zuständigen Behörden wahrnimmt. Dazu kommen spannende Fragestellungen im strafprozessualen Bereich, die in diesem Beitrag nur kurz andiskutiert werden konnten. Jedenfalls bilden die Bereiche Datenschutz, Digitalisierung und Strafprozessrecht ein Konglomerat an ungelösten Fragen, die es durch Zusammenarbeit von Wissenschaft und Praxis zu lösen gilt.

Datenschutz in der Justiz mit Blick auf das Strafverfahren

Mag. Kenan Ibili
Richter und Referent im Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz

I. Einleitung

Die wesentlichen Eckpunkte der Verordnung (EU) 2016/679[64] (Datenschutz-Grundverordnung; im Folgenden: DSGVO) und der Richtlinie (EU) 2016/680[65] (Datenschutzrichtlinie Polizei und Justiz; im Folgenden: DSRL-PJ) wurden in den vorangehenden Beiträgen dargestellt. Beide Rechtsakte gehen auf einen Vorschlag der Europäischen Kommission vom 25. Jänner 2012[66] zurück und verfolgen das Ziel, die 28 unterschiedlichen Datenschutzrechte der Mitgliedstaaten der Europäischen Union durch ein einheitlich geltendes europäisches Datenschutzrecht zu ersetzen bzw. zu harmonisieren.

Die DSRL-PJ, die im Vergleich zur DSGVO einen engeren Anwendungsbereich hat, zielt darauf ab, ein einheitliches, hohes Datenschutzniveau zu garantieren, um das Vertrauen zwischen den Polizei- und Justizbehörden in den verschiedenen Mitgliedstaaten zu stärken und damit zu einem freien Datenverkehr und einer wirksamen Zusammenarbeit

[64] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.
[65] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89.
[66] Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschluss und den Ausschuss der Regionen vom 25. Jänner 2012, KOM(2012) 9.

zwischen den Behörden beizutragen.[67] Beide Rechtsakte weisen viele Parallelen auf, die DSRL-PJ richtet sich allerdings nur an zuständige Behörden iSd Richtlinie (d.h. vor allem an Polizei- und Justizbehörden) und regelt bspw die Verarbeitung besonderer Kategorien personenbezogener Daten enger.[68] Der mindestharmonisierende Charakter der DSRL-PJ[69] ermöglicht es aber auch, weniger strenge Bereiche der DSRL-PJ zu verschärfen. Demgegenüber finden sich in der DSRL-PJ zudem speziellere Regelungen für den Strafbereich, wie sie in der DSGVO nicht vorgesehen sind. Solche wurden etwa in § 37 Abs 4 bis 9 DSG betreffend Datenkategorisierung (Beschuldigter, Opfer etc.) und Datenqualität umgesetzt.[70]

Trotz nationaler Begleitregelungen (DSG iHa die DSGVO) sowie konkreter Umsetzungsmaßnahmen (3. Hauptstück des DSG iHa die DSRL-PJ) war bislang dennoch mit keinem Rechtsakt der Europäischen Union eine so große Anpassungsnotwendigkeit in verschiedenen Materiengesetzen verbunden. Die Anpassungen im Bereich der Justiz finden sich im (ersten) Materien-Datenschutz-Anpassungsgesetz 2018, das Änderungen in mehr als 120 Gesetzen, angefangen vom Bundesarchivgesetz bis zum Weingesetz 2009, umfasst. Diesem lag für den Bereich der Justiz der ME Datenschutz-Anpassungsgesetz Justiz 2018[71] zugrunde, der von 21. Februar 2018 bis 13. März 2018 einer Begutachtung unterzogen wurde. In Kraft getreten sind die meisten Bestimmungen des ersten Datenschutzpakets[72] (insb. jene im Justizbereich) gemeinsam mit dem im Vorjahr beschlossenen Datenschutz-Anpassungsgesetz 2018[73] am 25. Mai 2018.[74]

---

[67] ErwG 7 DSRL-PJ.
[68] Art 10 DSRL-PJ, Art 9 DSGVO.
[69] Art 1 Abs. 3 DSRL-PJ.
[70] In Umsetzung der Art 6 und 7 DSRL-PJ.
[71] 16/ME 26. GP.
[72] BGBl. I Nr. 32/2018 (Materien-Datenschutz-Anpassungsgesetz 2018).
[73] BGBl. I Nr. 120/2017.
[74] Weitere Änderungen im DSG erfolgten zwischenzeitlich auf der Grundlage von zwei Initiativanträgen:

— Datenschutzgesetz - DSG, Änderung, BGBl. I Nr. 2018/23 (188/A), wonach die Zuständigkeit der Datenschutzbehörde neben jener zur Kontrolle der Vollziehung der in Art 19 B-VG bezeichneten obersten Organe auf den Bereich der Parlamentsverwaltung,

Besondere Aufmerksamkeit wurde medial vor allem der Strafbefugnis der nationalen Aufsichtsbehörden – in Österreich ist dies die Datenschutzbehörde[75] – geschenkt. Mit der Diskussion über die europaweite „Datenschutzwende“ wurde ein wichtiges Ziel erfüllt: Sensibilisierung des Schutzes personenbezogener Daten und Generalprävention. Für Behörden gilt die Strafbefugnis der Datenschutzbehörde nicht.[76]

Mit dieser Neugestaltung ist seit dem Regierungswechsel auch das Justizministerium neu strukturiert: Die Datenschutzbehörde und die für das Datenschutzgesetz zuständige Fachabteilung sind nunmehr im Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz (BMVRDJ) angesiedelt.[77] § 19 DSG idF des Datenschutz-Anpassungsgesetzes 2018,[78] wonach sich der Bundeskanzler vom Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten lassen kann, war als „Relikt“ der früheren Organisationsstruktur geschuldet. Diese Bestimmung wurde daher mit dem Datenschutz-Deregulierungs-Gesetz 2018[79] an die aktuelle Organisationsstruktur im BMVRDJ angepasst.

Im Folgenden soll überblicksweise aufgezeigt werden, wie die DSRL-PJ im nationalen Recht umgesetzt wurde **(Punkt II.)**. Danach sollen Abgrenzungsfragen der DSRL-PJ und der DSGVO im spezifischen Bereich der Justiz behandelt werden **(Punkt III.)**. Abschließend sollen die nationalen Anpassungen in

---

der Verwaltungsangelegenheiten des Rechnungshofes und der Volksanwaltschaft sowie der Justizverwaltung beim Verwaltungsgerichtshof erweitert wurde (§ 35 Abs. 2 DSG);

— Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 2018/24 (189/A), wonach nunmehr ua. klargestellt wurde, dass die Bestimmungen der Datenschutz-Grundverordnung sowie des Datenschutzgesetzes lediglich für die Verarbeitung personenbezogener Daten natürlicher Personen – und nicht auch juristischer Personen – gelten.

[75] §§ 18 Abs. 1, 31 Abs. 1, 36 Abs. 2 Z 15 DSG.

[76] Eine entsprechende Klarstellung erfolgte im Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 2018/24 (189/A), wonach gegen Behörden und öffentliche Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts keine Geldbußen verhängt werden können (§ 30 Abs. 5 DSG).

[77] § 2 Abs. 1 Z 2 iVm Anhang Teil 2 Abschnitt K Z 1 Bundesministeriengesetz 1986 in der Fassung der Bundesministeriengesetz-Novelle 2017, BGBl. I Nr. 164/2017.

[78] BGBl. I Nr. 120/2017.

[79] BGBl. I Nr. 24/2018.

der Strafprozeßordnung 1975 (StPO)[80] dargestellt werden **(Punkt IV.)**.

II. Umsetzung der DSRL-PJ

Nach Art 59 DSRL-PJ wird die Vorgängerregelung der DSRL-PJ, der Rahmenbeschluss 2008/977/JI[81], mit Wirkung vom 6. Mai 2018 aufgehoben. Der im strafrechtlichen Bereich vor Inkrafttreten des Vertrags von Lissabon erlassene Rahmenbeschluss 2008/977/JI galt bisher nur für die grenzüberschreitende Datenverarbeitung (Datenaustausch) und wurde innerstaatlich im DSG 2000 umgesetzt.

Mit dem Papier *„Der Schutz der Privatsphäre in einer vernetzten Welt. Ein Europäischer Datenschutzrahmen für das 21. Jahrhundert“* vom 25. Jänner 2012 machte die Europäische Kommission bereits in ihrem Vorschlag zu einer europäischen Datenschutzreform auf die aus ihrer Sicht geänderten Herausforderungen aufmerksam. So verfolgte sie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen das Ziel, einen überarbeiteten EU-Datenschutzrahmen sowohl für die grenzübergreifende, als auch erstmals für die innerstaatliche Verarbeitung personenbezogener Daten in der Strafverfolgung, Strafvollstreckung oder zum Schutz von und zur Abwehr von Gefahren für die öffentliche Sicherheit in allen Mitgliedstaaten zu schaffen. Damit sollte bewusst über den Anwendungsbereich des Rahmenbeschlusses 2008/977/JI hinausgegangen werden[82], was gleichzeitig einen Eingriff in das nationale Strafverfahren bedeutete.[83] Das Bestreben der

---

[80] BGBl. Nr. 631/1975 (WV) idF BGBl. I Nr. 32/2018.

[81] Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl L 2008/350.

[82] Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschluss und den Ausschuss der Regionen vom 25. Jänner 2012, KOM(2012) 9, S 10.

[83] Die Strafgesetzgebung und das Strafverfahren fallen in die Zuständigkeit der Mitgliedstaaten, auch wenn ihr Recht von Bestimmungen des Unionsrechts in diesem Bereich berührt werden kann [vgl. insb. die Urteile vom 15. September 2011, Dickinger und Ömer (C-347/09, Rn. 31), sowie vom 6. Dezember 2011, Achughbabian (C-329/11, Rn. 33);

Europäischen Kommission war, die Unterschiede in den Rechtsvorschriften der Mitgliedstaaten zu verringern, was – von der Europäischen Kommission noch zurückhaltend formuliert – *„voraussichtlich dem umfassenden Schutz personenbezogener Daten zugute“* kommen sollte. Hintergrund war, dass auch die nunmehr mit der DSGVO aufgehobene Richtlinie 95/46/EG (Datenschutz-Richtlinie)[84] nach ihrem Art 3 Abs 2 ausdrücklich nicht für die Datenverarbeitung von Polizei und Strafjustiz galt. Mit dem Inkrafttreten des Vertrags von Lissabon und der Einführung einer neuen Rechtsgrundlage (Art 16 AEUV), womit die Datenverarbeitung durch Polizei und Justiz stärker unionsrechtlich verankert wurde, sah die Europäische Kommission mit Blick auf die Erklärung Nr. 21 im Anhang zur Schlussakte der Regierungskonferenz die Grundlage, ein einheitliches Datenschutzregime zu schaffen.[85]

Nachdem der Rahmenbeschluss 2008/977/JI im DSG 2000 umgesetzt war, erfolgte auch die Umsetzung der DSRL-PJ im neuen DSG in einem eigenen Hauptstück und nicht in den einzelnen Materiengesetzen (StPO, StVG, SPG, PStSG etc.).

In Umsetzung der DSRL-PJ regelt das 3. Hauptstück des DSG (§§ 36 ff DSG) die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs. Der Anwendungsbereich des DSG wurde entsprechend der bisherigen Rechtslage insoweit erweitert, als die Bestimmungen des 3. Hauptstücks auch auf Datenverarbeitungen anzuwenden

---

vgl. auch StN GA Saugmandsgaard Øe vom 3. Mai 2018, Ministerio Fiscal (C-207/16), Rn 95].

[84] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

[85] Erklärung 21 des Vertrags von Lissabon: „Die Konferenz erkennt an, dass es sich aufgrund des spezifischen Charakters der Bereiche justizielle Zusammenarbeit in Strafsachen und polizeiliche Zusammenarbeit als erforderlich erweisen könnte, in diesen Bereichen spezifische, auf Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gestützte Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr zu erlassen.“

sind, die nicht in den Anwendungsbereich des Unionsrechts fallen.[86] Teilweise sind in diesem Bereich jedoch auch die Bestimmungen der DSGVO von Bedeutung, sofern das 3. Hauptstück des DSG auf die anderen Hauptstücke des DSG oder die DSGVO verweist. Weiters werden bestehende Datenschutzstandards im DSG beibehalten, um das bewährte Datenschutzniveau des DSG 2000 nicht zu senken.[87] Wie schon nach der geltenden Rechtslage sollen die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen als leges speciales den allgemeinen Regelungen des DSG (insb des 3. Hauptstücks) vorgehen.[88] Während dieser Grundsatz im deutschen Bundesdatenschutzgesetz (BDSG) gesetzlich verankert ist[89], finden sich entsprechende Erwägungen im österreichischen Datenschutzgesetz (DSG) lediglich in den Materialien, und zwar mehrfach im Bericht des Verfassungsausschusses des Nationalrates.[90]

[86] AB 1761 BlgNR 25. GP 18 zu § 36 DSG (Datenschutz-Anpassungsgesetz 2018); vgl für Deutschland auch § 85 BDSG.
[87] Art 1 Abs. 3 DSRL-PJ sieht vor, dass zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden strengere Garantien festgelegt werden können; vgl auch AB 1761 BlgNR 25. GP 18 zu § 36 DSG (Datenschutz-Anpassungsgesetz 2018).
[88] AB 1761 BlgNR 25. GP 18 zu § 36 DSG (Datenschutz-Anpassungsgesetz 2018).
[89] § 1 Abs. 2 BDSG, wonach andere Rechtsvorschriften des Bundes über den Datenschutz vorgehen.
[90] AB 1761 BlgNR 25. GP 2, 4, 6, 18 (Datenschutz-Anpassungsgesetz 2018).

III. Abgrenzungsfragen DSRL-PJ und DSGVO in der Justiz

a) Justizielle Tätigkeit der Gerichte

Grundsätzlich findet das DSG – wie bisher schon das DSG 2000 – keine Anwendung auf Akte der Gesetzgebung und Akte der Gerichte im Rahmen ihrer „justiziellen Tätigkeit".[91] Diese schon im Datenschutz-Anpassungsgesetz 2018 enthaltenen Ausführungen wollte der Gesetzgeber mit dem Datenschutz-Deregulierungsgesetz 2018 dahingehend bekräftigen, als angedacht war, dass Datenverarbeitungen im Bereich der Gesetzgebung und Gerichtsbarkeit weiterhin vom Grundrecht auf Datenschutz (§ 1 DSG) erfasst sein sollen, allerdings weder die DSGVO noch die übrigen Bestimmungen des DSG auf Datenverarbeitungen im Bereich der (nationalen) Gesetzgebung und der justiziellen Tätigkeit der Gerichte anzuwenden sein sollen.[92] Da die entsprechende Änderung der Verfassungsbestimmung des § 1 DSG im Nationalrat aber auch im zweiten Anlauf nicht gelang, blieben die Erwägungen, die das DSG konkretisieren sollten, unberücksichtigt. Bemerkenswert ist in diesem Zusammenhang, dass die Begründung des (nunmehr ohne Verfassungsmehrheit beschlossenen) Abänderungsantrages ohne Erklärung nur noch auf eine Ausnahme für die Gesetzgebung abstellt, die justizielle Tätigkeit der Gerichte aber unberücksichtigt lässt.[93]

Tatsächlich ist – soweit ersichtlich auch in Deutschland – nicht unumstritten, inwieweit das datenschutzrechtliche Regime für die „justizielle Tätigkeit" gilt. Das Materien-Datenschutz-Anpassungsgesetz 2018 beantwortete diese Frage bereits dahingehend, dass Datenverarbeitungen im zivilgerichtlichen Verfahren vom sachlichen Anwendungsbereich der DSGVO und des DSG nicht ausgenommen sind.[94] Gleichzeitig hat der

---

[91] AB 1761 BlgNR 25. GP 4 zu § 4 DSG (Datenschutz-Anpassungsgesetz 2018).
[92] AB 98 BlgNR 26. GP 3ff (Datenschutz-Deregulierungs-Gesetz 2018), vgl. insb. die Feststellung des Verfassungsausschusses auf Seite 5 in Zusammenhalt mit den Ausführungen auf Seite 3.
[93] AA-10 26. GP 4 (Abänderungsantrag zum Datenschutz-Deregulierungsgesetz 2018).
[94] ErläutRV 65 BlgNR 26. GP 150 (Materien-Datenschutz-Anpassungsgesetz 2018); auch *Selmayr* in *Ehmann/Selmayr* DS-GVO Art 55 Rz 13; *Körffer in Paal/Pauly,* DS-GVO BDSG[2]*,* Art 55 Rz 5; vgl auch § 1 Satz 1 iVm § 2 Abs 1 BDSG, wonach öffentliche Stellen des

Gesetzgeber klargestellt, dass die justizielle Tätigkeit der Strafgerichte unter das 3. Hauptstück des DSG fällt.[95]

Was von der justiziellen Tätigkeit konkret umfasst ist, bedarf einer autonomen Auslegung.[96] Weder in der DSGVO noch in der DSRL-PJ ist die justizielle Tätigkeit definiert. Auch in den Gesetzesmaterialien zum DSG fehlen entsprechende Leitlinien. Der Begriff „justizielle Tätigkeit" findet sich im DSG in zwei Bereichsausnahmen: Zum einen sind Gerichte im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen[97]; zum anderen ist die Datenschutzbehörde für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig.[98] Sinn und Zweck der Bereichsausnahme für die Gerichte ist in diesem Fall die Gewährleistung der richterlichen Unabhängigkeit, damit „die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt".[99] Der Begriff „justizielle Tätigkeit" wird davon ausgehend so verstanden, dass er die eigentliche rechtsprechende gerichtliche Tätigkeit umfasst[100] und sich zudem auf sämtliche

---

Bundes (auch Organe der Rechtspflege) und der Länder sowie nichtöffentliche Stellen unter das Regime des BDSG fallen; aA *Kühling/Martini* ua, DS-GVO und nationales Recht, 175f.

[95] Im Einklang mit FN 28 kann mE nichts anderes für die justizielle Tätigkeit der Strafgerichte gelten; deutlich auch ErläutRV 65 BlgNr 26. GP 164 (Materien-Datenschutz-Anpassungsgesetz 2018); auch *Dörnhöfer* in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), Seite 411; aA *Johannes/Weinhold* in *Das neue Datenschutzrecht bei Polizei und Justiz* Rz 21f, wonach Strafgerichte hinsichtlich der im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Datenverarbeitung der DSRL-PJ nicht unterliegen, wobei sie sich lediglich auf EG 80 und Art 45 Abs. 2 Satz 1 DSRL-PJ stützen, in denen vielmehr nur eine Ausnahme für die Zuständigkeit der Datenschutzbehörde geregelt ist. Die Diskussion über diese Abgrenzungsproblematik ist mE durch die subsidiäre Geltung des DSG in der StPO ohnehin entschärft und praktisch kaum von Bedeutung.

[96] Da die justizielle Tätigkeit in beiden Rechtsakten nicht definiert ist und insoweit auf die Rechtsordnungen der Mitgliedstaaten abzustellen ist, könnte fraglich sein, ob es sich überhaupt um einen autonomen Begriff des Unionsrechts handelt, der somit vom Europäischen Gerichtshof zu definieren ist (vgl. Schlussanträge GA Saugmandsgaard Øe vom 3. Mai 2018, Ministerio Fiscal (C-207/16), Rn 93f).

[97] § 57 DSG in Umsetzung von Art 32 bis 34 DSRL-PJ sowie Art 37 Abs. 1 lit a DSGVO

[98] § 31 Abs. 1 DSG in Umsetzung von Art 45 Abs. 2 DSRL-PJ

[99] ErwG 20 DSGVO; ähnlich ErwG 80 DSRL-PJ, wo es schlicht heißt: „(…) damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben gewahrt bleibt (…)."

[100] *Heberlein* in *Ehemann/Selmayr,* Datenschutzgrundverordnung, Art 37 Rz 21.

Tätigkeiten erstreckt, die mit der Entscheidungsfindung (arg. „Beschlussfassung“) im notwendigen Zusammenhang stehen.[101]

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 in § 83 Abs 2 GOG national festgelegt, dass „[d]ie justizielle Tätigkeit der Gerichte […] alle Tätigkeiten [umfasst], die zur Erfüllung der Aufgaben in Angelegenheiten der ordentlichen Gerichtsbarkeit erforderlich sind“: Davon umfasst sind auch die in Senaten ausgeübte Justizverwaltung[102], Notare in ihrer Funktion als Gerichtskommissäre[103], Befundaufnahmen und Gutachtenserstattung der gerichtlich bestellten Sachverständigen[104] sowie der gerichtlich bestellten Dolmetscher[105] als Teil des gerichtlichen Beweisverfahrens. Ob Sachverständige und Dolmetscher justizielle Tätigkeiten ausüben, sodass sie einem Gericht „im Rahmen der justiziellen Tätigkeit“ zuzurechnen sind, muss im Einzelfall geklärt werden[106] und hängt mE sowohl von der tatsächlichen Verarbeitung als auch vom gerichtlichen Auftrag ab.[107] Sie unterliegen jedenfalls der Aufsicht der Datenschutzbehörde, wenn sie die Daten zu anderen Zwecken (Mustersammlung, steuerliche oder zivilrechtliche Aufbewahrung etc.) weiterverarbeiten. Insofern wird auch in Deutschland unter „justizieller Tätigkeit“ der Kernbereich der richterlichen Tätigkeit verstanden, insb. die Rechtsfindung sowie die zur Vorbereitung und Durchführung dienenden Handlungen (zB Erstellung von

---

[101] *Körffer* in *Paal/Pauly* DS-GVO BDSG[2], Art 55 Rz 5.
[102] ErläutRV 65 BlgNr 26. GP 150 (Materien-Datenschutz-Anpassungsgesetz 2018) iHa Art 87 Abs. 2 B-VG.
[103] Ebenda.
[104] Ebenda.
[105] ErläutRV 65 BlgNr 26. GP 153 zu § 85a GOG (Materien-Datenschutz-Anpassungsgesetz 2018).
[106] Stellungnahme der Datenschutzbehörde zum Datenschutz-Anpassungsgesetz Justiz 2018, 1/SN-16/ME 26. GP 3 zu § 85a GOG.
[107] Erlass vom 24. April 2018 über die allgemeine Gewährleistung des Datenschutzes im BMVRDJ und in den nachgeordneten Dienststellen (Datenschutz-Erlass), BMVRDJ-Pr6116/0006-III 3/2018, Seite 8.

Entscheidungsentwürfen, Stimmausübung, Notizen und Vermerke über Beratungen, Terminbestimmung und Ladung, prozessleitende Maßnahmen, Zeugen- und Sachverständigenvernehmung, sitzungspolizeiliche Maßnahmen, Protokollführung).[108] Dieses weite Verständnis soll zur Verfahrensverwirklichung beitragen.

Daraus folgt, dass nur in Bezug auf die justiziellen Tätigkeiten selbst weder ein Datenschutzbeauftragter notwendig noch die Datenschutzbehörde berechtigt ist, datenschutzrechtliche Bewertungen vorzunehmen. Ob diese Bereichsausnahmen auch für die Staatsanwaltschaften greifen, hängt von der zentralen Frage ab, ob die Staatsanwaltschaft eine „unabhängige Justizbehörde“ ist, die im Rahmen ihrer „justiziellen Tätigkeit“ personenbezogene Daten verarbeitet. Dazu wurden schon unterschiedliche Auffassungen vertreten, die in einem eigenen Abschnitt behandelt werden sollen.[109]

Die Bereichsausnahmen im Bereich der justiziellen Tätigkeit der Gerichte bedeutet nicht, dass der Unionsgesetzgeber von einer – gänzlichen – Unanwendbarkeit der DSGVO (und auch des 3. Hauptstücks des DSG) ausgeht.[110] Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollen besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften der DSGVO (und des DSG) sicherstellen bzw. „Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten“.[111] Das Erfordernis einer solchen „Selbstkontrolle der Justiz“ fand in den Verordnungstext selbst nicht Eingang[112] und findet sich ebenso wenig in den Erwägungsgründen der zeitgleich

---

[108] *Wieczorek* in *Kühling/Buchner* DS-GVO BDSG § 9 BDSG Rz 9ff.
[109] Ausführlicher dazu Punkt IV lit. c) zur Frage der Kontrolle der Datenschutzbehörde.
[110] *Selmayr* in *Ehemann/Selmayr,* DS-GVO, Art 55 Rz 13; vgl FN 28 und 29.
[111] ErwG 20 DSGVO sowie ErwG 20 und 80 DSRL-PJ, wobei in der DSRL-PJ im Unterschied zur DSGVO eine Selbstkontrolle der Justiz nicht gefordert wird, sondern nur eine unabhängige Überwachung iSd Art 8 GRC.
[112] Auch *Körffer* in *Paal/Pauly* DS-GVO BDSG[2] Art 55 Rz 6.

beschlossenen DSRL-PJ, was auch durch den bloßen Verweis auf Art 8 Abs 3 GRC, welcher allgemein eine Kontrolle durch eine unabhängige Stelle vorsieht, nicht ausreichend klargestellt wird. Grundsätzlich wird eine solche Kontrolle begrüßt, zumal Beschwerden gegen gerichtliche Datenverarbeitungen in der Praxis häufig vorkommen.[113] Die näheren Umstände, welche Daten Gerichte für welche Zwecke und in welchem Umfang ermitteln und auf welche Weise sie sie verarbeiten dürfen, sowie alle weiteren für die gerichtlichen Datenverarbeitungen geltenden Grundsätze werden ohnehin umfassend durch die von den Gerichten einzuhaltenden Verfahrensgesetze und die darauf beruhenden Verordnungen sowie die Vorschriften des GOG determiniert.[114] Die gerichtlichen Verfahrensgesetze, die darauf beruhenden Verordnungen und das GOG regeln die datenschutzrechtlichen Rechte und Pflichten für den Bereich der zivil- und strafgerichtlichen Verfahren somit abschließend.[115]

b) Monokratische Justizverwaltung

Von der justiziellen Tätigkeit (einschließlich der kollegialen Justizverwaltung) ist die monokratische Justizverwaltung der Staatsanwaltschaften, Gerichte und Justizanstalten zu unterscheiden, für die die DSGVO umfassend gilt, sodass hier insb. auch die Kontrolle der Datenschutzbehörde greift. Zur monokratischen Justizverwaltung zählen typische Verwaltungstätigkeiten, wie zB Personal- und Hausverwaltung, äußerer Geschäftsbetrieb, Materialbeschaffung, Ausbildung, aber auch Auskünfte zu wissenschaftlichen Zwecken.[116]

Während sich die Betroffenenrechte im Bereich des Zivil- und Strafverfahrens – wie im Materien-Datenschutz-

---

[113] Ebenda.
[114] ErläutRV 65 BlgNr 26. GP 149 zu § 83 GOG (Materien-Datenschutz-Anpassungsgesetz 2018).
[115] ErläutRV 65 BlgNr 26. GP 151 zu § 84 GOG (Materien-Datenschutz-Anpassungsgesetz 2018).
[116] *Wieczorek* in *Kühling/Buchner* DS-GVO BDSG § 9 BDSG Rz 11; *Selmayr* in *Ehmann/Selmayr* DS-GVO Art 55 Rz 14; *Dörnhöfer* in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) Seite 404.

Anpassungsgesetz 2018 festgelegt – nach den jeweiligen Verfahrensrechten richten,[117] greifen für die monokratische Justizverwaltung die umfassenden Betroffenenrechte nach der DSGVO. Eine Beschränkung der Betroffenenrechte für den Bereich der monokratischen Justizverwaltung auf Grundlage von Art 23 DSGVO erscheint per se nicht ausgeschlossen.

c) Zuständige Behörde iSd DSRL-PJ

Für die Datenverarbeitung ist jede staatliche Stelle verantwortlich, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig ist (sog. „zuständige Behörde“ iSd DSRL-PJ).[118] Auch andere Stellen können zuständige Behörde iSd DSRL-PJ sein, wenn ihnen hoheitliche Befugnisse für die genannten Zwecke übertragen wurden.[119]

Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden für andere Zwecke fällt in den Anwendungsbereich der DSGVO.[120] Die Frage, wer eine zuständige Behörde iSd § 36 Abs 2 Z 7 lit. a DSG ist, lässt sich für den Bereich der Justiz einfach beantworten: Zuständige Behörden sind demnach die Gerichte im Rahmen ihrer justiziellen Tätigkeit[121], die Staatsanwaltschaften (samt Kriminalpolizei) im Bereich der Strafrechtspflege sowie die mit dem Strafvollzug betrauten Stellen (nicht bloße Verwaltung).[122]

---

[117] § 84 GOG iVm Art 23 Abs 1 lit f DSGVO, § 85a Abs 1 GOG; vgl. zur grundrechtsrelevanten Abwägung ErläutRV 65 BlgNr 26. GP 150f zu § 84 GOG sowie 153f zu § 85a GOG (Materien-Datenschutz-Anpassungsgesetz 2018).
[118] Art 3 Abs 7 lit. a DSRL-PJ.
[119] Art 3 Abs 7 lit b DSRL-PJ.
[120] ErwG 12 DSRL-PJ.
[121] Zum Begriff der justiziellen Tätigkeit siehe ausführlich oben Punkt III. a.
[122] Ausgenommen jeweils monokratische Justizverwaltung (vgl oben Punkt III. b.); vgl. auch Erlass vom 24. April 2018 über die allgemeine Gewährleistung des Datenschutzes im BMVRDJ und in den nachgeordneten Dienststellen Seite 4ff (BMVRDJ-Pr6116/0006-III 3/2018) sowie Informationserlass vom 9. April 2018 der Generaldirektion für Strafvollzug Seite 5f (BMVRDJ-GD41501/0009-II 1/2018).

Der Anwendungsbereich des 3. Hauptstücks des DSG knüpft kumulativ sowohl an ein personales als auch an ein sachliches Kriterium an. Fraglich ist, ob Behörden außerhalb des Kernbereichs der (typischen) Strafverfolgung, wie zB die Landespolizeidirektion Wien bei der Führung des Strafregisters nach § 1 Abs 2 StRegG, als zuständige Behörden iSd § 36 Abs 2 Z 7 DSG anzusehen sind.

Der Landespolizeidirektion Wien obliegt die Führung des Strafregisters[123]; dieses dient gemäß § 1 Abs 1 StRegG der Evidenzhaltung strafgerichtlicher Verurteilungen. Das Strafregister dient somit nicht der Strafverfolgung, der Gefahrenabwehr oder der Strafvollstreckung iSd DSRL-PJ, sondern – wie das deutsche Bundeszentralregister – lediglich der Auskunftserteilung über erfolgte Verurteilungen.[124] Insofern ist das Strafregisteramt nicht als eine zuständige Behörde iSd § 36 Abs 2 Z 7 DSG zu beurteilen, sondern ist für die Verarbeitung solcher Daten Art. 10 DSGVO maßgeblich.[125]

Das bedeutet, dass Behörden und öffentliche Stellen in ihrem Kernbereich mit Aufgaben iSd des 3. Hauptstücks des DSG (zB Strafverfolgung) betraut sein müssen, um sie als zuständige Behörde iSd DSRL-PJ qualifizieren zu können. Maßgeblich ist dabei auch, dass die in Frage stehende öffentliche Stelle hoheitliche Befugnisse für Zwecke des 3. Hauptstücks ausübt.

IV. Datenschutz im Strafverfahren

a) Terminologie

Das neue Datenschutzregime (3. Hauptstück des DSG in Umsetzung der DSRL-PJ) bringt inhaltlich keine wesentlichen Änderungen für das Strafverfahren; vielmehr sorgten die ersten Vorschläge zur DSRL-PJ für die Befürchtung einer Senkung des Datenschutzes in Strafverfahren.[126] Bereits vor der

---

[123] § 1 Abs. 2 StRegG.
[124] *Weichert* in *Kühling/Buchner* Art 10 Rz 18 bereits zur deutschen Rechtslage.
[125] *Weichert* in *Kühling/Buchner* Art 10 Rz 8f; *Schiff* in *Ehmann/Selmayr* Art 10 Rz 4f.
[126] *Souhrada-Kirchmayer* in Jahrbuch Datenschutzrecht und E-Government 2012, 9.

Umsetzung der Richtlinie wurde vertreten, dass für die StPO keine wesentlichen Auswirkungen zu erwarten sind.[127] Ein Anliegen bei der Anpassung der datenschutzrechtlichen Vorschriften in der StPO war es daher, an der bisherigen Systematik festzuhalten und – wie schon bisher – die subsidiäre Geltung des DSG beizubehalten, damit einerseits weiterhin ein hoher Datenschutz gewährleistet und andererseits ein Ausgleich von Strafverfahrenszwecken und Datenschutz gefunden wird.

Im Rahmen der Anpassungen an das DSG wurden daher im Bereich der StPO vorwiegend terminologische Änderungen vorgenommen. Geändert haben sich wesentliche Begriffe wie „Verwenden“ (nunmehr: „Verarbeitung“), „Daten“ (nunmehr: „personenbezogene Daten“), „Datenanwendung“ (nunmehr: „Datenverarbeitung“), „sensible Daten“ (nunmehr: „besondere Kategorien personenbezogener Daten“) und „Auftraggeber“ (nunmehr: „Verantwortlicher“). Der Begriff der Verarbeitung umfasst – wie bisher – sämtliche Vorgänge (erheben, erfassen, ordnen, speichern, auslesen, abfragen, übermitteln, abgleichen etc.).[128] Für das Strafverfahren von besonderer Bedeutung sind besondere Kategorien personenbezogener Daten (§ 39 DSG), die den Begriff der sensiblen Daten ablösen. Im Unterschied zu sensiblen Daten sind davon explizit nunmehr auch genetische und biometrische Daten umfasst.[129]

Neu ist der Begriff „Pseudonymisierung“ in § 77 Abs 2 StPO. Darunter versteht man „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

[127] *Dörnhöfer*, Datenschutz im Strafverfolgungsbereich: Schnittstellen und Abgrenzungsfragen, in *Knyrim* (Hrsg) Datenschutz-Grundverordnung (2016) Seite 405.
[128] § 36 Abs 2 Z DSG.
[129] Vgl. zu den Voraussetzungen unten IV lit. b.

Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.[130]

Unverändert geblieben ist die Verfassungsbestimmung des § 1 DSG und somit der darin enthaltene Begriff der schutzwürdigen Geheimhaltungsinteressen. Die bisher einfachgesetzlichen Bestimmungen des §§ 8 und 9 DSG 2000 sind nunmehr unmittelbar in den Art 6 (Rechtmäßige Verarbeitung) und Art 9 (Verarbeitung besonderer Kategorien personenbezogener Daten) DSGVO geregelt. Dementsprechend schreibt das DSG schutzwürdige Geheimhaltungsinteressen begrifflich auch in § 63 DSG fort, der deren Verletzung unter Strafe stellt. Im Bereich des 3. Hauptstücks des DSG wurden spiegelbildlich zu den Art 6 und Art 9 DSGVO die Art 8 und Art 10 der DSRL-PJ in den §§ 37 bis 40 DSG umgesetzt, woraus sich zudem die Verletzung von schutzwürdigen Geheimhaltungsinteressen ergibt. Zusammengefasst ist festzuhalten, dass vom bisherigen Bedeutungsinhalt auszugehen ist, soweit die StPO weiterhin auf die schutzwürdigen Geheimhaltungsinteressen hinweist.

b) Verarbeitung personenbezogener Daten im Strafverfahren

i. Rechtsgrundlagen der Verarbeitung:

Kriminalpolizei, Staatsanwaltschaften und Gerichte verarbeiten zur Erfüllung von Aufgaben nach der Strafprozessordnung (§ 1 Abs 1 StPO) naturgemäß personenbezogene Daten, also Informationen über eine identifizierte oder identifizierbare natürliche Person (zB Name, Online-Kennung, Standortdaten etc.), die auch besondere Merkmale enthalten (zB kulturelle oder soziale Identität oder molekulargenetischen Analyse).[131]

Grundsätzlich dürfen personenbezogene Daten nach § 37 Abs 1 DSG – wie bisher – nur auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden (Z 1 leg. cit.); sie dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke

[130] Art 4 Z 4 DSGVO, § 36 Abs. 2 Z 5 DSG.
[131] §§ 36 Abs 2 Z 1, 38, 39 DSG.

erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden (Z 2 leg. cit.). Ferner ist ihre Verarbeitung auf den Zweck der Datenverarbeitung zu beschränken und darf nicht über diesen hinausgehen (Z 3 leg. cit.). Personenbezogene Daten müssen schließlich so verarbeitet werden, dass sie im Hinblick auf den Verarbeitungszweck im Ergebnis sachlich richtig und auf den neuesten Stand gebracht sind (Z 4 leg. cit.). Ihre Aufbewahrung in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, ist nur soweit zulässig, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist (Z 5 leg. cit.);[132] eine längere Aufbewahrungsdauer kann sich aber auch aus dem Gesetz ergeben (zB archivrechtliche Vorschriften).

Das 3. Hauptstück des DSG fordert in Umsetzung des Art 8 der DSRL-PJ als Grundvoraussetzung für die Rechtmäßigkeit der Verarbeitung eine gesetzliche Grundlage. Die Verarbeitung muss nach § 38 DSG für die Erfüllung einer Aufgabe für die Zwecke des § 36 Abs 1 DSG (d.h. für Tätigkeiten der Polizei- und Justizbehörden) erforderlich und verhältnismäßig sein; im Übrigen ist eine Verarbeitung (ohne explizite gesetzliche Grundlage) auch dann zulässig, soweit sie zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist.[133]

Für Kriminalpolizei, Staatsanwaltschaft und Gericht wurde bislang aus § 74 Abs 1 StPO idF BGBl. I Nr. 19/2004 abgeleitet, dass sie personenbezogene Daten verarbeiten dürfen. Eine allgemeine Rechtsgrundlage für die Verarbeitung war dagegen in der StPO nicht explizit verankert. In § 74 Abs 1 erster Satz StPO wurde daher die im DSG geforderte Rechtsgrundlage für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten geschaffen. Demnach dürfen Kriminalpolizei, Staatsanwaltschaft und Gericht im Rahmen ihrer Aufgaben die hierfür erforderlichen personenbezogenen Daten verarbeiten. Die offene Formulierung soll alle Ebenen (Bezirksgericht,

---

[132] § 37 DSG.

[133] Abgeleitet aus Art 10 lit b DSRL-PJ; vgl. AB 1761 BlgNR 25. GP 19 zu § 38 DSG (Datenschutz-Anpassungsgesetz 2018).

Landesgericht, Oberlandesgericht, Oberster Gerichtshof, Staatsanwaltschaft, Oberstaatsanwaltschaft, Generalprokuratur) sowie alle Bereiche (auch Tätigkeiten der durch Staatsanwaltschaft oder Gericht bestellten Sachverständigen und Dolmetscher) abdecken.

Wie bisher ist generell beim Verarbeiten personenbezogener Daten nach § 77 Abs 2 StPO dem Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5 StPO) Rechnung zu tragen. Der eingangs dargestellte Grundsatz der Verarbeitung nach Treu und Glauben schließt geheime Überwachungsmaßnahmen oder verdeckte Ermittlungen aber auch weiterhin nicht aus; derartige Eingriffe unterliegen jedoch – wie bereits in der StPO vorgesehen – einer strengen Verhältnismäßigkeitsprüfung.[134]

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach § 39 DSG zulässig, wenn sie unbedingt erforderlich ist, wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen wurden und die oben genannten allgemeinen Voraussetzungen zu § 38 DSG gegeben sind (idR, dass die Verarbeitung gesetzlich vorgesehen und zur Aufgabenerfüllung erforderlich und verhältnismäßig ist). Diese Voraussetzungen müssen kumulativ vorliegen. Alternativ ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn diese von der betroffenen Person offensichtlich selbst öffentlich gemacht wurden. Die in § 39 DSG geforderten wirksamen Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen stellen keine neuen Voraussetzungen dar, sondern finden sich schon in § 74 Abs 2 StPO, wonach die Behörden bei der Verarbeitung besonderer Kategorien, aber schon allgemein bei strafrechtlich relevanten personenbezogenen Daten angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der betroffenen Personen zu treffen haben. Die Bestimmung wurde aufgrund der Sensibilität und angesichts der relativ häufigen Notwendigkeit der Verarbeitung

[134] AB 1761 BlgNR 25. GP 19 zu § 37 DSG (Datenschutz-Anpassungsgesetz 2018); vgl. auch ErwG 28 DSRL-PJ.

solcher Daten zur strafprozessualen Aufgabenerfüllung – auch im Hinblick auf die Verfassungsbestimmung des § 1 Abs 2 zweiter Satz DSG – geschaffen, um Strafverfolgungsbehörden in einer besonderen Bestimmung nochmals auf die Notwendigkeit angemessener Vorkehrungen (zB Verschlüsselung der Datenübermittlung, Zugangsrestriktionen, entsprechende Schulungsmaßnahmen etc.) zur Wahrung der Geheimhaltungsinteressen der Betroffenen im Falle der Verarbeitung derartiger Daten hinzuweisen.[135]

ii. Die StPO als lex specialis:

Als datenschutzrechtliche Kernbestimmung im Strafverfahren soll in § 74 Abs 1 zweiter Satz StPO weiterhin der Grundsatz aufrechterhalten werden, dass die Bestimmungen des DSG (insb. das 3. Hauptstück) im Strafverfahren Anwendung finden und Ausnahmen nur dort bestehen, wo die StPO selbst Sonderregeln vorsieht. Das bedeutet, dass – soweit die StPO nicht ausdrücklich eine gesetzliche Ermächtigung für die Verarbeitung personenbezogener Daten vorsieht – die Zulässigkeit der Verarbeitung nicht nur nach den Regelungen der StPO, sondern auch in Bezug auf §§ 36ff DSG zu prüfen ist.[136] Allerdings soll im Unterschied zur alten Rechtslage darüber hinaus klargestellt werden, dass durch den Entfall der Wortfolge „im Einzelnen“ in § 74 Abs 1 StPO der Vorrang der StPO „generalisierend“ wirkt und sich nicht nur auf jene Konstellationen bezieht, in denen explizite Bestimmungen in der StPO bestehen.[137] Das bedeutet, wenn sich zu einem bestimmten Bereich eine Regelung in der StPO findet, diese das (möglicherweise auch weiterreichende) DSG ausschließt. In diesem Sinne soll die Abdeckung eines bestimmten Regelungsbereichs in der StPO zum Ausschluss der Anwendbarkeit des DSG führen, auch wenn der Umfang der in der StPO vorhandenen Bestimmungen ebenfalls unter den Vorgaben des DSG liegt. Eine solche subsidiäre Geltung des

---

[135] ErläutRV 25 BlgNR 22. GP 107.

[136] vgl. zur alten Rechtslage ErläutRV 25 BlgNR 22. GP 107; *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 2.

[137] ErläutRV 65 BlgNr 26. GP 164 zu § 74 StPO (Materien-Datenschutz-Anpassungsgesetz 2018).

DSG im Strafverfahren ist vom Gesetzgeber gewollt und im Bericht des Verfassungsausschusses des Nationalrates mehrfach gerade auch erwähnt.[138]

Wie bereits in der Literatur vertreten, wird die Auskunft innerhalb der StPO typischerweise über die Regelung der Akteneinsicht präzisiert. So übernimmt auch § 44 Abs 5 DSG die bisherige Regelung des § 26 Abs 8 DSG 2000 und stellt klar, dass das Akteneinsichtsrecht dem Auskunftsrecht vorgeht. Daneben bleibt kein Raum für das Auskunftsrecht nach dem DSG.[139] § 43 Abs 4 DSG sieht darüber hinaus vor, dass die Informationsverpflichtung nach dem DSG aufgeschoben, eingeschränkt oder entfallen kann, insb. zur Gewährleistung, dass die Ermittlung oder Verfolgung von Straftaten nicht beeinträchtigt werden und dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist; eine solche Abwägung nimmt die StPO im Hinblick auf Verständigungspflichten vor.

Zusammengefasst kann daher festgehalten werden, dass die Auskunfts- und Informationsrechte nach dem DSG nicht greifen, weil in der StPO ein ausgeglichenes Auskunfts- und Informationsrecht durch das Recht auf Akteneinsicht besteht und die Verständigungsverpflichtung aus der StPO das Informationsbedürfnis abdeckt (zB aus §§ 66 Abs 1 Z 3 iVm 70 Abs 1 oder §§ 138 Abs 5, 139 Abs 2 StPO). Ein darüber hinausgehendes Auskunfts- und Informationsrecht jeder sonst noch berührten Person (zB nicht verfahrensrelevante Namen bei zahlreichen Daten in Wirtschaftsverfahren) findet – auch unter Berücksichtigung des Verfahrensaufwandes – keine Rechtfertigung.[140] Auf die Möglichkeit des Akteneinsichtsrechts nach § 77 Abs 1 StPO sei an dieser Stelle nur hingewiesen.

---

[138] AB 1761 BlgNR 25. GP 2, 4, 6, 18 (Datenschutz-Anpassungsgesetz 2018).
[139] *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 74 Rz 60.
[140] Auf den Verfahrensaufwand stellt auch § 139 Abs. 2 StPO ab; vgl. auch § 24 Abs. 3 Z 3 DSG 2000.

c) Aufsichtsrechte der Datenschutzbehörde bei staatsanwaltschaftlicher Tätigkeit

Unter Punkt III a) wurde zusammengefasst ausgeführt, dass die Datenschutzbehörde für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig ist. Fraglich ist, ob die Staatsanwaltschaft aufgrund ihrer Weisungsbindung[141] eine „unabhängige Justizbehörde" iSd DSRL-PJ ist, weil nur solche in „ihrer justiziellen Tätigkeit" keiner Aufsicht unterliegen.

i. Die Staatsanwaltschaft als unabhängige Justizbehörde

Nach deutscher Lehrmeinung üben Staatsanwaltschaften und Kriminalpolizei bei Datenverarbeitungsvorgängen im Rahmen von Ermittlungsmaßnahmen (selbst bei gerichtlich bewilligten Ermittlungsmaßnahmen) keine justizielle Tätigkeit aus. Begründet wird dies damit, dass die Durchführung der Ermittlungsmaßnahme (auch bei gerichtlicher Anordnung) durch die Kriminalpolizei erfolge.[142] Auch in Österreich wird argumentiert, dass Staatsanwälte in Österreich trotz ihrer verfassungsrechtlichen Stellung als Organe der Gerichtsbarkeit keine „justizielle Tätigkeit" iSd DSRL-PJ ausüben würden, weil ihnen die in der DSRL-PJ geforderte Unabhängigkeit fehle.[143]

Grundsätzlich können die Mitgliedstaaten nach der DSRL-PJ auch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von der Zuständigkeit der Aufsichtsbehörde ausnehmen. Unter anderen unabhängigen Justizbehörden iSd Art. 45 Abs. 2 der DSRL-PJ sind insb Staatsanwaltschaften zu verstehen (vgl. den hier relevanten EG 80 DSRL-PJ). Staatsanwälte sind nach § 1 StAG *„zur Wahrung der Interessen des Staates in der Rechtspflege"* berufen und üben zwangsläufig eine justizielle Tätigkeit iSd DSRL-PJ aus, wobei dies nicht deckungsgleich mit der justiziellen Tätigkeit von

---

[141] Vgl. Art.90a B-VG, §§ 2, 29a ff StAG.
[142] *Wieczorek* in *Kühling/Buchner* DS-GVO BDSG § 9 BDSG, Rz 10.
[143] *Dörnhöfer* in *Knyrim* (Hrsg) Datenschutz-Grundverordnung (2016) Seite 411; vgl. auch die Stellungnahme der Datenschutzbehörde zum Datenschutz-Anpassungsgesetz Justiz 2018, 1/SN-16/ME 26. GP 5.

Gerichten sein muss. Dies ergibt sich schon aus der Wortfolge des § 45 Abs. 2 zweiter Satz DSRL-PJ, wonach „*andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit*“ von der Aufsicht der Datenschutzbehörde ausgenommen werden können. Damit wird durch den Unionsgesetzgeber zuerkannt, dass es andere Justizbehörden geben kann, die eine andere Art der justiziellen Tätigkeit ausüben - wie beispielsweise Staatsanwaltschaften - wobei Sinn und Zweck einer Bereichsausnahme in diesem Fall nicht ist, die richterliche Unabhängigkeit zu schützen, sondern deren Eigenschaft als unabhängige Justizbehörde zu wahren. Dies wird auch durch EG 80 dritter Satz DSRL-PJ deutlich, der im Hinblick auf andere Justizbehörden (Staatsanwaltschaften) nicht auf die Unabhängigkeit der Richter abzielt. Die DSRL-PJ betrachtet Justizbehörden und Gerichte näher, indem sie beide Begriffe in Zusammenhang setzt (EG 20). Die Richtlinie legt fest, dass andere Justizbehörden lediglich im Rahmen ihrer justiziellen Tätigkeit Gerichten gleichgestellt sind (EG 63). Sie spricht unabhängige Justizbehörden (Staatsanwaltschaften; vgl EG 80) im Rahmen ihrer justiziellen Tätigkeit an, ohne konkret festzulegen, wie diese Unabhängigkeit ausgestaltet sein soll.

Mit diesen Erwägungen möchte der Unionsgesetzgeber mE jedenfalls nicht, dass ein Äquivalent zu strengen richterlichen Garantien geschaffen werden soll, wenn von einer Justizbehörde gesprochen wird. Eine solche Gleichsetzung mit Gerichten würde die Frage aufwerfen, wieso eine Abgrenzung zu Justizbehörden überhaupt besteht. Was den Kernbegriff der „unabhängigen Justizbehörde“ betrifft, so ist mE in Zusammenschau mit anderen Rechtsakten auch auf das bestehende autonome Begriffsverständnis zurückzugreifen.[144]

Die justizielle Tätigkeit von Justizbehörden findet – anders als andere strafrechtliche Rahmenbeschlüsse und Richtlinien – in der DSRL-PJ explizit Erwähnung, um die Justizverwaltung von der (justiziellen) Tätigkeit der Justizbehörden abzugrenzen.

[144] Vgl zum Begriff der Justizbehörde, die auch Staatsanwaltschaften umfasst, Art 2 der Richtlinie 2014/41/EU; EG 47 der Richtlinie 2016/800/EU; EG 38 der Richtlinie 2013/48/EU.

Damit soll zum Ausdruck gebracht werden, dass nur Verwaltungsagenden der Aufsicht der Aufsichtsbehörde unterliegen. Wie oben festgehalten, sind Staatsanwälte zur Mitwirkung in der Rechtspflege berufen und somit justiziell tätig.

Im Ergebnis könnte der Schluss gezogen werden, dass die Staatsanwaltschaft eine unabhängige Justizbehörde ist, die auch justiziell iSd DSRL-PJ tätig ist. Anzumerken ist, dass sich die Mitwirkung der Staatsanwaltschaft in der Rechtspflege auch nicht durch eine ministerielle Weisung ändert. Der Staatsanwalt trägt nämlich – als Organ der Gerichtsbarkeit – selbst im Falle einer Weisung die Verantwortung für die Ermittlungen. Die Handlungen des Staatsanwalts werden dadurch insb nicht zu einem Akt der Verwaltung.[145] Fraglich ist daher im Kern, ob eine andere Justizbehörde iSd DSRL-PJ, die in der Rechtspflege mitwirkt, die gerichtsgleiche Unabhängigkeit aufweisen muss.

Diese Frage muss an dieser Stelle offengelassen werden; spannend bleibt freilich, wie der EuGH diese in einem allfälligen Vorabentscheidungsverfahren beantworten wird.

ii. Datenschutzbehörde im Ermittlungsverfahren

Im Datenschutz-Anpassungsgesetz 2018[146] wurde eine Bereichsausnahme für die Staatsanwaltschaft in § 31 Abs. 1 DSG gesetzlich nicht explizit verankert. Es wurde jedoch im DSG eine Lösung im Bereich des Rechtsschutzes geschaffen, was eine (organisatorische) Zuständigkeit der DSB nach § 31 DSG nicht notwendig machen sollte. Zu untersuchen ist, ob diese Aussage im Bereich des Rechtsschutzes auch zutrifft.

Unstrittig ist, dass der Datenschutzbehörde als nationale Aufsichtsbehörde keine Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zukommt.[147] Zusätzlich dazu wurde in den Materialien zum Datenschutz-Anpassungsgesetz 2018

---

[145] *Wiederin*, in *Fuchs/Ratz* [Hrsg.], Wiener Kommentar zur StPO, § 4 Rn. 52 und 53.
[146] BGBl. I Nr. 120/2017.
[147] § 36 Abs 1 DSG.

festgehalten, dass die Bestimmungen über die Aufgaben der Datenschutzbehörde nach § 32 DSG – in den Fällen der Z 4, 5 und 8 – im Bereich der StPO nicht anwendbar sind.[148] Aus dieser ausdrücklichen Ausnahme für die StPO im DSG ist zu schließen, dass die Datenschutzbehörde im Anwendungsbereich der StPO keine Beschwerden einer betroffenen Person untersuchen (Z 4), die Rechtmäßigkeit von Verarbeitungen prüfen (Z 5) sowie die Rechte der betroffenen Person wahrnehmen soll (Z 8). Hintergrund dieser Ausnahme ist, dass es in diesen Fällen ohnedies einen gerichtlichen Rechtsschutz gibt. Typischerweise kann nach der StPO mit Einspruch wegen Rechtsverletzung, Beschwerde oder Nichtigkeitsbeschwerde/Berufung gegen das Urteil vorgegangen werden, um Datenschutzverletzungen geltend zu machen. Erst wo diese Möglichkeiten enden, besteht darüber hinaus subsidiärer Rechtsschutz nach dem GOG.[149]

Demnach kommen der Datenschutzbehörde auch im Bereich der staatsanwaltlichen Ermittlungstätigkeit keine Untersuchungsbefugnisse zu, weil durch den Einspruch wegen Rechtsverletzung nach § 106 StPO letztlich eine gerichtliche Kontrolle des staatsanwaltlichen Handelns möglich ist (§§ 106 Abs 5, 107 Abs 3 StPO). Entspricht die Staatsanwaltschaft dem Antrag des Einspruchswerbers und kommt es in weiterer Folge auch nicht zur gerichtlichen Kontrolle (§ 106 Abs 4 StPO), ist der rechtmäßige Zustand schon hergestellt. Nur dort, wo ein Rechtsschutz im Ermittlungsverfahren nach § 106 StPO nicht gegeben ist, könnte mE eine Kontrollbefugnis der Datenschutzbehörde bestehen, wie zB im Hinblick auf selbstständige Akte der Kriminalpolizei, wenn eine Genehmigung nach § 99 Abs 2 StPO nicht vorliegt.[150]

---

[148] AB 1761 BlgNR 25. GP 17 (Datenschutz-Anpassungsgesetz 2018).
[149] *Reindl-Krauskopf* in *Fuchs/Ratz*, WK-StPO § 74 Rz 67.
[150] Bei einem selbstständigen polizeilichen Akt besteht zwar auch eine gerichtliche Kontrolle durch das Landesverwaltungsgericht, allerdings sehen die Erläuterungen nur eine generelle Ausnahme zum Aufgabenbereich der Datenschutzbehörde „im Bereich der StPO“ vor, sodass solche selbstständigen Akte idR außerhalb davon sind.

Allerdings vertrat die Datenschutzbehörde im Rahmen des Begutachtungsverfahrens zum ME Datenschutz-Anpassungsgesetz Justiz 2018 die Ansicht, dass sie, ungeachtet einer gerichtlichen Zuständigkeit, zur inhaltlichen Behandlung einer allfälligen Beschwerde gegen eine Entscheidung der Staatsanwaltschaft zuständig sei. Sie wies allgemein darauf hin, dass die Staatsanwaltschaft weder als Gericht noch als unabhängige Justizbehörde iSd Art 45 Abs 2 DSRL-PJ angesehen werden könne und folglich von der Zuständigkeit der Datenschutzbehörde nicht ausgenommen sei.

In diesem Zusammenhang ist jedoch hervorzuheben, dass die Frage der Zuständigkeit der Datenschutzbehörde über die Aufsicht außerhalb der justiziellen Tätigkeit (§ 31 zweiter Satz DSG) getrennt von der Frage zu betrachten ist, ob ihr tatsächlich Aufgaben in diesem Bereich zukommen. Es kann nicht ungeachtet gelassen werden, dass die Untersuchungsbefugnisse der Datenschutzbehörde nach § 33 DSG im Anwendungsbereich des § 36 Abs 1 DSG nur in ihrem jeweiligen Aufgabenbereich bestehen. Im DSG ist vom Aufgabenbereich der Datenschutzbehörde – wie oben ausgeführt – der Bereich der StPO bewusst ausgenommen. Diese Ausnahme ist also von § 31 DSG unabhängig und diese daher ergänzend zu sehen; sie gründet allein auf dem Umstand, dass nach der StPO ohnedies ein umfassender gerichtlicher Rechtsschutz greift, sodass die Datenschutzbehörde nicht kontrollierend eingreifen muss. Daher gilt die zitierte Ausnahme auch im Bereich der von § 31 DSG nicht umfassten Staatsanwaltschaften, egal ob es sich um einen (dem Einspruch nachgeordneten) gerichtlichen Rechtsschutz nach der StPO oder den einer Beschwerde nach dem GOG nachgeordneten Rechtsschutz handelt, weil jedenfalls ein solcher Rechtsschutz möglich ist.

Dies wird letztlich dadurch unterstützt, dass im DSG keine explizite Koexistenz von gerichtlichen Rechtsbehelfen vorgesehen ist.[151] Damit soll primär die Gefahr

[151] Vgl auch Art 78, 79.

widersprechender gerichtlicher Entscheidungen in derselben Sache vermieden werden. Sie soll aber auch zur Rechtssicherheit beitragen. Die Auffassung der Datenschutzbehörde würde mit dem Zuständigkeitskonzept des DSG in Angelegenheiten des Rechtsschutzes in Widerspruch stehen. § 27 Abs 1 DSG sieht nämlich nur die Möglichkeit der Beschwerde beim Bundesverwaltungsgericht (gegen Bescheide der Datenschutzbehörde) vor und soll damit offenkundig auch den nach Art 79 DSGVO bzw. Art 54 DSRL-PJ einzuräumenden gerichtlichen Rechtsbehelf gegen Verantwortliche und Auftragsverarbeiter abdecken. Das DSG sieht daher nur einen einzigen gerichtlichen Rechtsbehelf bei Datenschutzverletzungen vor und möchte gerade keinen parallelen gerichtlichen Rechtschutz bei Datenschutzverletzungen gewähren. Während die Datenschutzbehörde ihre Zuständigkeit im Bereich der DSGVO unmittelbar aus der DSGVO ableiten kann, ist dies im Bereich des DSG (in Umsetzung der DSRL-PJ) nicht zulässig. Daraus ist zu schließen, dass die Datenschutzbehörde ihre Zuständigkeit nicht bejahen kann, weil sich daraus die Konsequenz ergeben würde, dass über ihre Bescheide nach §§ 34 Abs 5 iVm 27 Abs 1 DSG das Bundesverwaltungsgericht entscheiden würde. Da es im Rahmen der StPO aber ohnehin einen gerichtlichen Rechtsbehelf bei Datenschutzverletzungen gibt, erübrigt sich eine Kontrolle durch die Datenschutzbehörde.

d) Akteneinsicht nach § 77 Abs 2 StPO

Die Akteneinsicht nach § 77 Abs 2 StPO regelt, unter welchen Voraussetzungen in einem Strafverfahren rechtmäßig erhobene personenbezogene Daten für Zwecke wissenschaftlicher Forschung von Forschungseinrichtungen verarbeitet werden dürfen. Sie geht zudem als lex specialis den allgemeinen Datenschutzvorschriften vor (§ 74 Abs 1 StPO).

Folgende Voraussetzungen müssen nach § 77 Abs 2 StPO vorliegen:

1. Primär müssen personenbezogene Daten pseudonymisiert werden;
2. Nur dann, wenn die personenbezogenen Daten
    a. nicht oder nur mit einem unverhältnismäßigen Aufwand pseudonymisiert werden können und
    b. das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Geheimhaltungsinteresse der betroffenen Person erheblich überwiegt,

ist die Übermittlung personenbezogener Daten durch Erteilung von Auskünften, Einsicht in Akten eines Verfahrens und Herstellung von Abschriften zu gewähren.

Nach dem Wortlaut des § 77 Abs 2 StPO erfolgt die Übermittlung der Daten idR durch Auskunftserteilung. Nur wenn dadurch der Zweck der Forschungsarbeit nicht erreicht werden kann oder die Erteilung einen unverhältnismäßigen Aufwand erfordert, kann daneben Akteneinsicht gewährt werden. In der Praxis ist die Akteneinsicht die Regel und die Auskunftserteilung naturgemäß die Ausnahme. Wird Akteneinsicht gewährt, können die Akten (sofern diese elektronisch verfügbar sind auch in dieser Form) zur Einsichtnahme zur Verfügung gestellt werden. Als seltene Form kennt die Regelung noch die Möglichkeit der Herstellung von Abschriften.

Die Akteneinsicht nach § 77 Abs 2 StPO ist nur zulässig, wenn das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Geheimhaltungsinteresse der betroffenen Person an dem Ausschluss der Einsicht zu solchen Zwecken erheblich überwiegt. Es ist daher eine sorgfältige Abwägung des vom Antragsteller hinreichend darzulegenden öffentlichen Interesses an der Forschungsarbeit einerseits und des schutzwürdigen Geheimhaltungsinteresses der betroffenen Person andererseits vorzunehmen.[152] Besonders zu

[152] ErläutRV 65 BlgNR 26. GP 166 zu § 77 Abs 2 StPO (Materien-Datenschutz-Anpassungsgesetz 2018).

berücksichtigen ist das öffentliche Interesse (Arg. „erheblich überwiegt“), wobei nicht jede Forschungsarbeit ein öffentliches Interesse begründen muss. Es sind auch Forschungsarbeiten denkbar, die rein von wissenschaftlicher Bedeutung sind. Im Bereich des Strafrechts sind Forschungsarbeiten jedoch in aller Regel von öffentlichem Interesse.

Anhang:

DSGVO – Fit in 10 Schritten

Dr. Gerald Ganzger
Rechtsanwalt

SCHRITT 1
Erhebung des Status der derzeitigen Datenverarbeitung

Im Wesentlichen ist zu erheben:

- Welche Daten werden verarbeitet?
- Wie werden diese Daten bzw. auf welcher Rechtsgrundlage werden diese Daten erhoben bzw. gesammelt?
- Wie und wie lange werden diese Daten aufbewahrt?
- Wohin und an wen werden Daten weitergegeben?

SCHRITT 2
Einrichtung eines Datenschutz-Compliance-Systems

- Erstellung des Verzeichnisses der Verarbeitungstätigkeiten
- Erstellung einer Datenschutzstrategie/Datenschutz-Policy
- Festlegung der Verantwortlichkeiten für die Verpflichtungen nach DSGVO, insbesondere für die Wahrung der Betroffenenrechte
- Festlegung von Abläufen bei Anfragen/Anträgen von betroffenen Personen

SCHRITT 3
Bestellung eines Datenschutzbeauftragten

- Ist auch dann sinnvoll, wo ein solcher nicht zwingend vorgeschrieben ist
- Entscheidung, ob extern oder intern
- Datenschutzbeauftragte für Filialbetriebe

SCHRITT 4
Überprüfung der Datenschutzzustimmungserklärungen

- Entsprechen diese noch der Rechtslage
- Wie werden diese dokumentiert
- Anpassung von AGB

SCHRITT 5
Überprüfung der bisher verwendeten Formulare /
Herstellen der erforderlichen Urkunden

- Werden im Betrieb einheitliche Formulare verwendet?
- Sind frühere Formulare vernichtet worden?
- Welche Formulare werden in Filialbetrieben verwendet?
- Datenschutzerklärung
- Anpassung der Dienstverträge

SCHRITT 6
Errichtung eines Kontrollsystems

- Wer ist für die Kontrolle verantwortlich?
- Was wird kontrolliert?
- Wie erfolgen Stichproben?

SCHRITT 7
Einrichtung eines Dokumentationssystems

- Sammeln/Verwahren der Datenschutzzustimmungserklärungen
- Aufbewahrung der Datenschutz-Folgenabschätzungen
- Interne Anweisungen
- Anträge von Betroffenen und die Erledigung der Anträge
- Dokumentation von Kontrollen

- Dokumentation von Schulungen

SCHRITT 8
Überprüfung der Verträge mit Auftragsverarbeitern

- Welche Verträge gibt es?
- Sind die Verantwortlichkeiten DSGVO-konform geregelt?

SCHRITT 9
Datenschutz durch Technik

- Implementierung von technischen Compliance-Maßnahmen
- Es ist zu evaluieren, ob technische Maßnahmen zu ergreifen sind, z.B. Pseudonymisierung
- Implementierung von verpflichtenden Datensicherheitsmaßnahmen (Artikel 32)

SCHRITT 10
Information der Mitarbeiter und Schulungen

- Informationen an Mitarbeiter sollen den Aufgabenbereichen der jeweiligen Mitarbeiter entsprechen
- Dokumentation der Information
- Schulungen und Vermerk dieser im Personalakt