universität wien

MASTERARBEIT

Titel der Masterarbeit

„Datentransfer ins Ausland –

Eine Bestandsaufnahme zur Datenschutz-Grundverordnung der Europäischen Union und die Analyse ihrer Änderungen“

Verfasser

Mag. Martin Führer

angestrebter akademischer Grad

Master of Laws (LL.M.)

Wien, 2014

Universitätslehrgang:	Informations- und Medienrecht
Studienkennzahl lt. Studienblatt:	A 992 942
Betreuer:	a.o. Univ. Prof. Dr. Dietmar Jahnel

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch, JGS 946/1811 idF BGBl I 33/2014
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BGBl	Bundesgesetzblatt
bzw	beziehungsweise
dh	das heißt
DSAV	Datenschutzangemessenheits-Verordnung, BGBl. II Nr. 521/1999 idF BGBl. II Nr. 213/2013
DSG	Datenschutzgesetz 2000, BGBl I 165/1999 idF BGBl I 83/2013
DS-GVO	Datenschutzgrundverordnung; gegenständlich in der Version des vom Ausschuss des Europäischen Parlamentes für bürgerliche Freiheiten, Justiz und Inneres (LIBE) am 21.11.2013 eingereichten Entwurfs für die Europäische Datenschutz-Grundverordnung
DSRL	Datenschutzrichtlinie, RL 95/46/EG
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
ff	fortfolgende
Hrsg	Herausgeber (-in)
idF	in der Fassung
iSd	im Sinne des/der
iVm	in Verbindung mit

LIBE-Ausschuss	Ausschuss des Europäischen Parlamentes für bürgerliche Freiheiten, Justiz und Inneres
lit	litera
maW	mit anderen Worten
mMn	meiner Meinung nach
OGH	Oberster Gerichtshof
zB	zum Beispiel

Einleitung

Die Europäische Union unterzieht die europäischen Datenschutzvorschriften derzeit einer umfassenden Novellierung. Das gesamte europäische Datenschutzrecht befindet sich daher aktuell im Umbruch. Kernstück der bereits seit mehreren Jahren vorbereiteten Datenschutzreform wird eine neue Verordnung, die Datenschutz-Grundverordnung, sein.

Mit dieser – in den Mitgliedsstaaten direkt anwendbaren – Verordnung werden nicht nur inhaltliche Neuerungen, sondern auch ein Systemwechsel verbunden sein. Das bisherige Zusammenspiel einer europäischen Richtlinie mit einer Vielzahl an nationalen Umsetzungsgesetzen wird zukünftig im allgemeinen Datenschutzrecht nicht mehr existieren. Stattdessen sollen durch die Datenschutz-Grundverordnung nicht nur Auslegungs- und Umsetzungsschwierigkeiten hintangehalten, sondern auch durch Beseitigung der einzelnen nationalen – naturgemäß unterschiedlichen – Datenschutzgesetze ein einheitliches europäisches Datenschutzniveau geschaffen werden.

Eine Verabschiedung der Datenschutz-Grundverordnung vor dem Jahr 2015 ist zwar aus heutiger Sicht unrealistisch, dennoch eignet sich der derzeit vorliegende Entwurf aufgrund der sich abzeichnenden Tendenzen bereits jetzt für eine nähere Durchleuchtung. Wiewohl im Rahmen der anstehenden Trialog-Verhandlungen Änderungen in den Detailfragen und Formulierungen als wahrscheinlich gelten, soll die gegenständliche Masterthesis zum ehest möglichen Zeitpunkt die sich abzeichnenden Neuerungen aufzeigen und deren Auswirkungen im Vergleich zu den bisherigen Vorschriften analysieren. Am Ende soll eine Beurteilung der neuen rechtlichen Rahmenbedingungen und des daraus zu erwartenden Schutzniveaus stehen, die es erlaubt und ermöglicht, selbst bei inhaltlichen Änderungen durch den derzeit laufenden Europäischen Gesetzgebungsprozess als Basiswerk herangezogen zu werden.

Um den zur Verfügung stehenden Rahmen sinnvoll nutzen zu können, bietet sich anstatt der Behandlung sämtlicher Neuerungen eine Eingrenzung auf einen Teilbereich an. Beweggrund für die Auswahl des Datentransfers ins Ausland als zu bearbeitenden Themenkreis waren folgende Überlegungen: Derzeit kann eine unabhängig vom laufenden Gesetzgebungsprozess zur Datenschutz-Grundverordnung stattfindende Sensibilisierung von Gesellschaft, Wirtschaft und Politik im und für den Bereich des Datenschutzes vernommen werden. Mitverantwortlich dafür war neben den aktuellen Entwicklungen in der Gesetzgebung auch eine Vielzahl an globalen Ereignissen.

Zunächst führte die durch das so genannte Whistleblowing[1] und die Enthüllungen von Edward Snowden[2] ausgelöste Überwachungsaffäre jedenfalls zu einer Erhöhung des Drucks auf die europäische Politik, wirksame Abwehrmaßnahmen gegen unzulässige Datensammlung und -verwendung zu setzen. In diese Bestrebungen reihen sich die jüngsten Aufforderungen des EU-Parlaments an die EU-Kommission zum Widerruf der Safe-Harbor-Erklärung gegenüber den Vereinigten Staaten von Amerika ein. Die EU-Kommission forderte in diesem Zusammenhang im Herbst 2013 von der US-Regierung Nachbesserungen in 13 Punkten. Derzeit dürften die Vereinigten Staaten dem Großteil der Forderungen entsprechen, jedoch bleibt abzuwarten, wie die Reaktion in den zentralen Punkten – vor allem im Bereich der Geheimdienstaktivitäten – aussehen wird. Aufgrund der enormen Folgen für die Zulässigkeit bzw. Genehmigungspflicht des Datentransfers in die USA als – in dieser Hinsicht wichtigstem – Drittstaat stellt dies eine weitere überaus spannende Frage im Rahmen des gegenständlichen Themenkreises dar.

Auch in der Rechtsprechung spiegeln sich die aktuellen Entwicklungen wider, zuletzt durch die Anrufung des EuGH durch den Irish High Court.[3] Dieser ersuchte den EuGH mit Urteil vom 18.06.2014 um Beantwortung der Vorlagefrage, ob die in der Europäischen Charta der Grundrechte garantierten Rechte auf Privatsphäre und Datenschutz mit amerikanischen Standards im Einklang stehen – und zwar unabhängig von der Safe-Harbour-Erklärung und insbesondere mit Blick auf die Programme der Vereinigten Staaten zur Massenüberwachung.

All diese jüngsten Entwicklungen haben ihre gemeinsame Grundlage im grenzüberschreitenden Datenverkehr, insbesondere jenem in Drittstaaten. Nicht zufällig daher die eingangs erwähnte Sensibilisierung der europäischen Gesellschaft, deren Misstrauen in Datenverarbeitungen umso höher ist, je weiter entfernt (räumlich, sprachlich und gedanklich) diese stattfindet. Verstärkt wird dieses Empfinden durch die Korrelation mit dem zumeist geringeren Datenschutzniveau im verarbeitenden Staat und/oder Empfängerstaat.

Den diesbezüglichen Neuerungen in der Datenschutz-Grundverordnung und deren Auswirkungen auf den Schutz von über die Mitgliedsstaats- bzw. EU-Grenzen hinaus transferierten Daten wird daher verstärkte Beachtung zukommen. Dies alles rechtfertigt eine nähere Betrachtung des Themenkreises *„Datentransfer ins Ausland“*.

---

[1] Definition laut deutschem Online-Verwaltungslexikon olev.de: „Alarm schlagen" bei Missständen: Weitergabe von Information über und Kritik an illegalem oder unethischen Verhalten in einer Institution durch Insider, uneigennützig und trotz persönlicher Risiken.

[2] Ehemaliger Mitarbeiter der US-amerikanischen Geheimdienste CIA (Central Intelligence Agency) und NSA (National Security Agency).

[3] Vgl (Irish) High Court, 2013, No. 765JR.

Die Arbeit wird dabei zunächst die geltende österreichische Rechtslage beleuchten und anschließend die korrelierenden Regelungen der derzeit aktuellen Version der Datenschutzgrundverordnung – allenfalls unter Berücksichtigung der zwischenzeitlichen Änderungen im Vergleich zum Entwurf der Europäischen Kommission – analysiert. Um möglichst strukturiert an die derzeit bewegliche Materie heranzugehen, wird die Arbeit in die beiden Teilbereiche (i) Datentransfer ins EU-Ausland und (ii) Datentransfer in Drittstaaten aufgeteilt.

Aktuelle Fassung

Aufgrund des noch laufenden Gesetzgebungsverfahrens, steht der endgültige Text der Datenschutz-Grundverordnung noch nicht fest. Umso mehr ist es notwendig, genau festzulegen, auf welcher Fassung die gegenständliche Arbeit aufbaut. Die Europäische Kommission initiierte das Gesetzgebungsverfahren mit dem Vorschlag an das Europäische Parlament und den Rat vom 25.01.2012.[4] Am 21.11.2013 reichte der Ausschuss des Europäischen Parlamentes für bürgerliche Freiheiten, Justiz und Inneres (LIBE) seinen Entwurf für die Europäische Datenschutz-Grundverordnung ein, der im Vergleich zur Ausgangsversion der Europäischen Kommission in zahlreichen Punkten bedeutende Änderungen aufwies.

Dieser Entwurf wurde am 12.03.2014 von den Abgeordneten des Europäischen Parlamentes akzeptiert und dient als Grundlage für die Trialog-Verhandlungen zwischen Europäischem Parlament, Europäischer Kommission und dem Rat der Europäischen Union. Ebenso bildet diese Version der Datenschutz-Grundverordnung, wie sie sich nach Passieren der 1. Lesung des Europäischen Parlaments zeigt, die Basis für die Analysen in der gegenständlichen Arbeit. Sofern im Rahmen dieser Arbeit die Datenschutz-Grundverordnung, ihre Kurzform *„DS-GVO“* oder die Bezeichnung *„LIBE-Entwurf“* erwähnt sind, wird auf diese Fassung Bezug genommen.

An manchen Stellen werden die Entwicklungen seit dem und die Änderungen im Vergleich zum letzten Entwurf der Europäischen Kommission bearbeitet. Dieser Entwurf der Kommission – KOM (2012) 11 endg. – wird im Rahmen der Arbeit als *„Kommissionsentwurf“* bezeichnet.

[4] KOM (2012) 11 endg.

Geschlechtsneutralität

Um eine bessere Lesbarkeit zu erreichen, wurde auf geschlechtsneutrale Formulierungen verzichtet. Es versteht sich jedoch von selbst, dass sich alle personenbezogenen Bezeichnungen auf beide Geschlechter beziehen.

1. Aktuelle Rechtslage

Aktuell geltendes Regelungsregime für den Themenkomplex *„Datentransfer ins Ausland“* stellen die Datenschutzrichtlinie der Europäischen Union und deren nationale Umsetzungsgesetze – in Österreich das Datenschutzgesetz 2000 (kurz *„DSG“*) – dar.

Das DSG stellt ebenso wie die europarechtlichen Vorgaben grundsätzlich nur personenbezogene Daten unter seinen Schutzbereich. Sofern daher im Rahmen dieser Arbeit ohne nähere Angaben von *„Daten“* gesprochen wird, sind damit ausschließlich personenbezogene Daten gemeint.

1.1. Anzuwendendes Recht

Aufgrund der momentanen Konstellation, die je Mitgliedsstaat ein nationales Umsetzungsgesetz bedingt, entfaltet der grenzüberschreitende Datenverkehr automatisch Berührungspunkte mit einer oder mehreren verschiedenen Rechtsordnungen. Sowohl innerhalb der EU als auch beim Datentransfer in Drittstaaten stellt sich daher in aller Regel zunächst die Frage nach dem anzuwendenden Recht.

Das DSG ist zunächst auf jede Datenverarbeitung im Inland anzuwenden, folgt insofern dem Territorialitätsprinzip.[5] Darunter fallen jedenfalls alle rein innerstaatlichen Sachverhalte wie auch Sachverhalte, bei denen internationale Unternehmen Daten aus dem EU-Ausland zumindest teilweise in Österreich verarbeiten.[6] Hat jedoch ein Auftraggeber seinen Sitz in einem anderen EU-Mitgliedsstaat, gleichzeitig aber keine Niederlassung[7] in Österreich, kommt selbst bei einer Verarbeitung in Österreich dessen innerstaatliches Recht zur Anwendung. Voraussetzung dafür ist, dass die Daten auch zum Zweck dieser österreichischen Niederlassung verarbeitet werden.[8] Umgekehrt bedeutet diese – als lex specialis anzusehende – Ausnahme zugunsten des Sitzstaatsprinzips aber auch, dass im Falle eines österreichischen Auftraggebers, der in einem anderen Mitgliedsstaat eine Datenverarbeitung betreibt ohne dort für die Verfolgung seiner Interessen eine Niederlassung zu besitzen, österreichisches Datenschutzrecht – diesfalls im EU-Ausland – zur Anwendung gelangt.[9]

---

[5] § 3 Abs 1 1. Satz DSG.
[6] *Dörnhöfer*, Datenschutz bei Grenzüberschreitungen, in Jahnel (Hrsg), Datenschutzrecht und E-Government, Jahrbuch 2012, 59.
[7] ISd § 4 Z 14 DSG.
[8] § 3 Abs 2 DSG.
[9] Erläuterungen zur Regierungsvorlage zur Stammfassung DSG 2000: ErlRV 1613 BlgNR XX. GP.; *Pollirer/Weiss/Knyrim*, DSG. Datenschutzgesetz² § 3 (2014).

Nun ist Inhalt der gegenständlichen Arbeit die Beleuchtung des Datentransfers aus Sicht eines Österreichischen Auftraggebers ins Ausland. Im Lichte der obigen Ausführungen kommt bei den dabei denkbaren Konstellationen stets österreichisches Datenschutzrecht zur Anwendung. Dies auch wegen der in Artikel 25 und 26 der EU-Datenschutzrichtlinie[10] (im Nachfolgenden *„DSRL"*) normierten Einschränkungen für die Übermittlung personenbezogener Daten in Drittländer. Damit soll eine Umgehung europäischer Mindeststandards durch eine Datenverwendung in Drittstaaten ausgeschlossen werden. Das führt jedoch zu einer sehr geringen Schwelle, die für die Anwendbarkeit von österreichischem (beziehungsweise jeweiligem nationalen) Datenschutzrecht zur erreichen ist. Beispielsweise ist nach Ansicht der Artikel-29-Datenschutzgruppe nationales Datenschutzrecht des Mitgliedsstaates bereits dann anzuwenden, wenn Webseiten von Auftraggebern aus Drittländern Cookies verwenden, um Daten von Festplatten auszulesen, die sich auf einem PC in diesem Mitgliedsstaat befinden.[11]

1.2. Sachlicher Anwendungsbereich

Die DSRL schützt natürliche Personen bei der Verarbeitung personenbezogener Daten und definiert diese folglich in konsequenter Weise als alle Informationen über eine bestimmte oder bestimmbare natürliche Person.[12] Insofern umfasst der Schutzbereich des DSRL nur Daten von natürlichen Personen. Das österreichische DSG hingegen unterscheidet in der Begriffsdefinition des Betroffenen nicht zwischen natürlicher und juristischer Person, erwähnt sogar beide gleichzeitig und ausdrücklich.[13] Folglich sind auch die personenbezogenen Daten juristischer Personen vom sachlichen Anwendungsbereich umfasst und geht dieser somit erheblich über jenen der DSRL hinaus.[14]

1.3. Vorgaben aus dem Unionsrecht

An dieser Stelle darf zunächst darauf hingewiesen werden, dass die bereits in der Datenschutzrichtlinie verwendeten Begriffe des *„für die Verarbeitung Verantwortlichen"*[15]

---

[10] 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 idF L 2003/284, 1.

[11] *Artikel-29-Datenschutzgruppe,* Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU vom 30.05.2002, WP 56, 5035/01/DE/endg., 11 <www.cnpd.public.lu/de/publications/groupe-art29/wp056_de.pdf> (24.08.2014).

[12] Art 2 lit. a DSRL.

[13] § 4 Z 3 DSG.

[14] *Dörnhöfer* in Jahnel, Datenschutzrecht und E-Government, Jahrbuch 2012, 59.

[15] Art 2 lit d DSRL.

und des *„Auftragsverarbeiters“*[16] im österreichischen Datenschutzgesetz mit den Begriffen *„Auftraggeber“* [17] und *„Dienstleister“* [18] übersetzt wurden.[19] Im Rahmen der Behandlung der aktuellen Rechtslage daher das letztere Begriffspaar verwendet.

Die DSRL regelt entsprechend ihrer Konzeption den Datenverkehr zwischen den Mitgliedsstaaten nicht gesondert, gibt jedoch die Grundlagen für die Zulässigkeit einer Übermittlung von personenbezogenen Daten in Drittländer vor.

Das dabei verwendete Grundsätze-Ausnahmen-Modell legt zunächst in Artikel 25 DSRL den Mitgliedsstaaten die Pflicht auf, Regelungen zu treffen, wonach eine Übermittlung von Daten in Drittstaaten (nur) dann zulässig ist, *„wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet“*[20]. Die weiteren Absätze des Artikel 25 DSRL ermächtigen die Europäische Kommission zur Feststellung, welchem Drittland ein angemessenes Datenschutzniveau zugebilligt wird.

Ist kein angemessenes Schutzniveau im Empfängerstaat gegeben, ist bei Verwirklichung eines der Ausnahmetatbestände des Artikel 26 DSRL eine Übermittlung dennoch zulässig. In Frage kämen etwa die ausdrückliche Einwilligung des Betroffenen [21], die Notwendigkeit der Übermittlung zur Erfüllung eines Vertrages oder ausreichende Garantien des Auftraggebers hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten des Betroffenen.[22]

1.4. Nationale Umsetzung – Die Vorschriften des Datenschutzgesetzes

Artikel 25 und 26 DSRL wurden in Österreich durch die §§ 12 und 13 DSG umgesetzt. Diese beiden Bestimmungen legen fest, unter welchen Voraussetzungen ein Datentransfer ins Ausland einer vorherigen Genehmigung durch die Datenschutzbehörde (kurz *„DSB“*) bedarf bzw. in welchen Fällen eine Weitergabe von Daten genehmigungsfrei vollzogen werden kann.

---

[16] Art 2 lit e DSRL.
[17] § 4 Z 4 DSG.
[18] § 4 Z 5 DSG.
[19] Zur Abgrenzung: Stellungnahme 1/2010 der Artikel-29-Datenschutzgruppe vom 16.02.2010, 00264/10/DE, WP 169 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf> (24.08.2014).
[20] Art 25 (1) DSRL.
[21] § 4 Z 3 DSG.
[22] Vgl Art 26 (2) DSRL.

1.4.1. Grundvoraussetzungen für die Zulässigkeit

Den nachstehenden Abwägungen, ob im Einzelfall eine Genehmigung der DSB eingeholt werden muss oder nicht, sei vorangestellt, dass jedenfalls – als Grundvoraussetzung – eine Genehmigungsfreiheit nur dann gegeben sein kann, wenn die Datenverwendung, wäre sie im Inland gelegen, rechtmäßig und zulässig wäre.[23] Aus diesem Grund ist zunächst in pointierter Form auf die jeweiligen Zulässigkeitsvoraussetzungen der jeweiligen Art der Datenweitergabe einzugehen.

Die österreichische Rechtsordnung differenziert zwischen zwei verschiedenen Arten der Datenweitergabe, die sich in der Person des Empfängers unterscheiden. Im DSG haben sich dafür durch die Legaldefinition die Begriffe *„Überlassen“*[24] und *„Übermitteln“*[25] etabliert. Überlassen von Daten beschreibt gemäß § 4 Z 11 DSG die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen eines Auftragsverhältnisses. Unter einer Übermittlung ist die Weitergabe von Daten *„an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister“*[26] zu verstehen.

a. Übermittlung von Daten

Im Falle einer Übermittlung von Daten müssen die Voraussetzungen der §§ 7ff DSG erfüllt sein.[27] Die Begriffsdefinition[28] sieht als Übermittlung von Daten

- die Weitergabe von Daten an Dritte
- die Veröffentlichung von Daten und
- die Verwendung von Daten für ein anderes Aufgabengebiet als jenes des Auftraggebers

an. Entsprechend § 7 Abs 2 DSG ist Grundvoraussetzung für die Zulässigkeit einer Datenübermittlung, dass die Daten bereits aus einer zulässigen Datenverwendung stammen. Die Darstellung der umfassenden Prüfung der Zulässigkeit einer Datenverwendung und des dabei anzuwendenden Prüfungsschemas steht nicht im unmittelbaren Fokus dieser Arbeit und

[23] § 12 Abs 5 DSG.
[24] § 4 Abs 11 DSG.
[25] § 4 Abs 12 DSG.
[26] § 4 Z 12 DSG.
[27] Vgl *Jahnel*, Handbuch Datenschutzrecht (2010), Rz 4/133.
[28] § 4 Z 12 DSG.

würde deren Rahmen sprengen. Diesbezüglich darf auf die zahlreiche einschlägige Literatur verwiesen werden.[29]

Darüber hinaus müssen folgende Voraussetzungen erfüllt sein:

Erstens muss der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht haben.[30] Vor allem bei Standardanwendungen und den dort vorgesehenen Empfängerkreisen wird – für den Behördenbereich[31] – die Zuständigkeit bzw Befugnis außer Zweifel stehen.[32] Ansonsten bilden die Gewerbeberechtigung, eine sonstige Berufsberechtigung (zB Eintragung in die Rechtsanwaltsliste) oder im Banken- und Telekommunikationsbereich die jeweilige gesetzlich notwendige Konzession Anhaltspunkte für die rechtliche Befugnis des Empfängers.[33] Unterschiedlich beurteilt die Literatur die Frage, ob bei bestimmten Datenarten – zu denken ist etwa an bereits zulässigerweise veröffentlichte oder indirekt personenbezogene Daten – überhaupt eine Glaubhaftmachung notwendig sein soll. Während etwa *Jahnel* keine Privilegierung dieser Datenarten sieht und daher die Notwendigkeit einer Glaubhaftmachung nur im Falle einer zweifellos gegebenen Befugnis verneint,[34] wird diese Privilegierung – offenbar aus praktischen Überlegungen – anderenorts bejaht.[35] Im Gesetz jedenfalls findet die Privilegierung bestimmter Datenarten – obwohl das DSG an anderen Stellen[36] sehr wohl darauf Rücksicht nimmt – keine Deckung.

Zweitens muss gewährleistet sein, dass durch den Zweck und den Inhalt der Datenübermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.[37] Die Rechtfertigungsgründe, wann diese Interessen des Betroffenen nicht verletzt sind, finden sich für nicht-sensible Daten in § 8 DSG und für sensible Daten[38] in § 9 DSG. Auch eine nähere Darstellung dieser Rechtfertigungsgründe kann vom Fokus und vom Rahmen der gegenständlichen Arbeit nicht umfasst sein, weshalb mit einem Verweis auf die Ausführungen der Literatur das Auslangen gefunden werden muss.[39] An dieser Stelle sei

---

[29] Ausführlich zB *Jahnel*, Handbuch Datenschutzrecht, Rz 4/7 ff.
[30] § 7 Abs 2 Z 2 DSG.
[31] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/124.
[32] *Pollirer/Weiss/Knyrim*, DSG. Datenschutzrecht² § 7 Anm 9 (2014).
[33] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/16.
[34] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/123.
[35] *Pollirer/Weiss/Knyrim*, DSG. Datenschutzrecht² § 7 Anm 9 (2014).
[36] So etwa § 12 Abs 3 Z 2 DSG.
[37] § 7 Abs 2 Z 3 DSG.
[38] § 4 Z 2 DSG.
[39] Siehe etwa *Jahnel*, Handbuch Datenschutzrecht, Rz 4/19 ff.

jedoch angemerkt, dass für nicht-sensible Daten – wenn keine Zustimmung des Betroffenen zur Datenverarbeitung vorliegt – in der Regel eine Rechtfertigung über eine positive Interessensabwägung zu Gunsten des Übermittlenden oder die Notwendigkeit der Datenübermittlung zur Vertragserfüllung gefunden werden wird. [40] Diese beiden Rechtfertigungsgründe stehen im Regime der 13 Rechtfertigungsgründe des § 9 DSG jedoch nicht zur Verfügung. Für sensible Daten wird daher – wenn nicht einer der 12 anderen, in der Praxis jedoch eher selteneren Rechtfertigungsgründen erfüllt ist – die ausdrückliche Zustimmung des Betroffenen einzuholen sein.[41]

Selbst wenn sämtliche der obigen Voraussetzungen erfüllt sind, ist die Datenübermittlung (als gewöhnliche Datenverwendung) nur dann zulässig, wenn die durch sie verwirklichten Eingriffe in das Grundrecht auf Datenschutz[42] nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgt sind sowie zusätzlich die Grundsätze des § 6 DSG eingehalten wurden.[43]

Zudem muss jede Datenübermittlung – als Eingriff in das Grundrecht auf Datenschutz – selbst bei Zulässigkeit nach dem einfachgesetzlichen Teil des DSG [44] zusätzlich auch den Voraussetzungen des § 1 Abs 2 DSG entsprechen.[45] Daher muss einer der vier in § 1 Abs 2 DSG normierten Fälle, in denen ein Grundrechtseingriff zulässig ist, nämlich

- die Verwendung im lebenswichtigen Interesse des Betroffenen,
- die Verwendung mit Zustimmung des Betroffenen,
- die Verwendung zur Wahrung überwiegender berechtigter Interessen eines anderen bei Eingriffen einer staatlichen Behörde oder
- die Verwendung zur Wahrung überwiegender berechtigter Interessen eines anderen bei anderen Eingriffen

auch bei Datenübermittlungen verwirklicht sein.[46]

b. Überlassen von Daten

Wie auch bei der Übermittlung bedingt eine zulässige Überlassung von Daten an einen Dienstleister zunächst eine bereits zulässige Datenverwendung durch den die Daten

[40] § 8 Abs 1 Z 4 und Abs 3 Z 4 DSG.
[41] § 9 Z 6 DSG.
[42] § 1 DSG.
[43] § 7 Abs 3 DSG.
[44] §§ 4 – 64 DSG.
[45] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/131.
[46] Zu den Voraussetzungen der vier möglichen Fälle: *Jahnel*, Handbuch Datenschutzrecht, Rz 2/33 ff.

überlassenden Auftraggeber. Zudem werden sowohl dem Auftraggeber (in § 10 DSG) als auch dem Dienstleister (in § 11 DSG) zusätzliche Pflichten auferlegt.

Auftraggeber dürfen demnach bei ihren Datenanwendungen (nur dann) Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Die entsprechenden Vereinbarungen hat der Auftraggeber mit dem Dienstleister abzuschließen sowie deren Einhaltung zu überprüfen.[47] Eine Zustimmung des Betroffenen ist nicht notwendig, § 10 Abs 1 DSG allein normiert die Berechtigung der Inanspruchnahme von Dienstleistern.[48] Jedoch ist aus der Formulierung des § 10 Abs 1 1. Satz DSG eine Prüfpflicht des Auftraggebers abzuleiten, in dessen Rahmen sich der Auftraggeber primär die entsprechende Gewerbeberechtigung des Dienstleister vorweisen lassen müssen wird.[49] Das Einholen weiterer Nachweise, wie etwa das Vorliegen von Standesregeln, denen der Dienstleister unterliegt, kann bei entsprechend sensiblen Daten indiziert sein. Je sensibler die betreffenden Daten, desto sorgfältiger wird ein Auftraggeber der Frage nachzugehen haben, wie weit ein in Aussicht genommener Dienstleister als geeignet im Sinne des § 10 DSG angesehen werden kann, bzw welche Verpflichtungen einem solchen Dienstleister – vor einem datensicherheitstechnischen Hintergrund – vertraglich auferlegt werden müssen.[50]

Beabsichtigt der Auftraggeber die Inanspruchnahme von Dienstleistern im Rahmen einer der Vorabkontrolle iSd § 18 Abs 2 DSG unterliegenden Datenverwendung, hat er dieses Vorhaben der DSB mitzuteilen. Dies gilt jedoch nur, wenn die Heranziehung nicht aufgrund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder nicht Dienstleister herangezogen werden sollen, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis stehen. [51] Beispielsweise ist der Hauptverband der Sozialversicherungsträger gemäß § 31 Abs 11 ASVG in jenen Fällen, in denen er auf Grund gesetzlicher Bestimmungen für die Versicherungsträger tätig wird, Dienstleister für die Versicherungsträger.[52] Nach einer entsprechenden Mitteilung hat die DSB zu prüfen, ob durch die Heranziehung die schutzwürdigen Interessen des Betroffenen beeinträchtigt werden können, und gegebenenfalls dies dem Auftraggeber mitzuteilen. Der Auftraggeber ist zwar nicht verpflichtet, einer negativen Stellungnahme der DSB zu folgen, jedoch kann die DSB in weiterer Folge in Form einer Empfehlung nach § 30 Abs 6 DSG vorgehen und zur Sicherung

[47] § 10 Abs 1 DSG.
[48] DSK 03.09.2002, K211.413/006-DSK/2002.
[49] *Pollirer/Weiss/Knyrim*, DSG. Datenschutzrecht² § 10 Anm 3 (2014).
[50] DSK 03.09.2002, K211.413/006-DSK/2002.
[51] § 10 Abs 2 DSG.
[52] *Dohr/Pollirer/Weiss/Knyrim*, DSG. Datenschutzrecht² § 10 Anm 7 (16. ErgLfg 2014).

der Einhaltung dieser Empfehlung die in den Z 1 bis 3 leg cit genannten Mitteln anwenden.[53] Darunter fällt die Möglichkeit zur Verwaltungsstrafanzeige oder bei schwerwiegenden Verstößen durch Auftraggeber (große Anzahl von Betroffenen, intensive oder wiederholte Angriffe auf die geschützten Bereiche, Beeinträchtigung des öffentlichen Interesses)[54] das Recht zur Erhebung einer Feststellungsklage [55] beim zuständigen Gericht sowie bei Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ (Bundesminister, Landesregierung bzw. zuständige Landesrat)[56] mit der Empfehlung zu befassen.[57]

Die Pflichten des Dienstleisters wiederum werden in § 11 Abs 1 Z 1 bis 6 DSG normiert und bestehen bereits kraft Gesetzes, bedürfen daher keiner weiteren vertraglichen Vereinbarung.[58] Erst die nähere Ausgestaltung dieser Pflichten muss zum Zweck der Beweissicherung schriftlich festgehalten werden.[59]

Dem Dienstleister obliegt daher jedenfalls die Pflicht, die Daten ausschließlich im Rahmen der Aufträge zu verwenden und zu übermitteln,[60] alle gemäß § 14 DSG erforderlichen Datensicherheitsmaßnahmen zu treffen,[61] weitere Dienstleister nur mit Billigung des Auftraggebers hinzuzuziehen,[62] im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen,[63] nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, entweder dem Auftraggeber zu übergeben oder diese in dessen Auftrag weiter aufzubewahren oder zu vernichten,[64] sowie dem Auftraggeber jene Informationen zur Verfügung zu stellen, die dieser zur Kontrolle der Einhaltung der obigen Pflichten benötigt.[65]

Bei Überlassungen ins Ausland muss neben der Voraussetzungen der §§ 10 f DSG zudem eine schriftliche Zusage des empfangenden Dienstleisters vorliegen, mit welcher dieser dem Übermittelnden bestätigt, dass er die Dienstleisterpflichten nach § 11 Abs 1 DSG einhalten

---

[53] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 3/58.
[54] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 30 Anm 22.
[55] § 32 Abs 5 DSG.
[56] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 30 Anm 23.
[57] Vgl § 30 Abs 6 Z 3 DSG.
[58] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 11 Anm 3.
[59] § 11 Abs 2 DSG.
[60] § 11 Abs 1 Z 1 DSG.
[61] § 11 Abs 1 Z 2 DSG.
[62] § 11 Abs 1 Z 3 DSG.
[63] § 11 Abs 1 Z 4 DSG.
[64] § 11 Abs 1 Z 5 DSG.
[65] § 11 Abs 1 Z 6 DSG.

werde.[66] Diese Zusage ist auch bei Überlassung an einen Dienstleister im EWR-Vertragsraum notwendig,[67] obwohl eine solche keiner speziellen Genehmigung der Datenschutzbehörde bedarf.[68] Lediglich dann, wenn die Dienstleistung im Ausland – egal ob EU-Mitgliedstaat oder Drittland – in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, kann die schriftliche Zusage entfallen.[69]

1.4.2. Genehmigungsfreier Datentransfer

a. Generell genehmigungsfreier Datentransfer

Angelehnt an Artikel 26 Abs 1 DSRL regelt das DSG in § 12 Abs 3 – in taxativer Aufzählung – Tatbestände, bei deren Erfüllung ein Datentransfer ins Ausland jedenfalls als genehmigungsfrei anzusehen ist. In diesen Fällen ist es unerheblich, in welchen Empfängerstaat die Daten überlassen oder übermittelt werden.

So ist etwa der Transfer von Daten genehmigungsfrei, die bereits im Inland zulässigerweise veröffentlicht,[70] sohin einem weiten Personenkreis zugänglich gemacht wurden.[71] Gleiches gilt bei indirekt personenbezogenen Daten.[72] Darunter sind Daten zu verstehen, bei denen der Personenbezug für den Auftraggeber, den Dienstleister oder den Empfänger der Übermittlung mit rechtlich zulässigen Mitteln nicht herstellbar ist.[73] Ein Rückschluss auf die Identität des Betroffenen darf dabei bloß aus rechtlichen Gründen nicht möglich sein, das Erreichen eines bestimmten – allenfalls technischen – Schwierigkeitsgrades ist nicht erforderlich.[74] Schließlich wurde – wie an anderen Stellen[75] im DSG – auf die Zustimmung des Betroffenen abgestellt. Liegt diese hinsichtlich des Datentransfers ins Ausland vor und ist beweisbar, dass der Betroffene in voller Kenntnis der Tragweite zugestimmt hat, ist die Übermittlung oder Überlassung ebenfalls genehmigungsfrei.[76]

Zudem bedarf der Datentransfer ins Ausland jedenfalls auch dann keiner Genehmigung, wenn er in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht Gesetzesrang haben

---

[66] § 12 Abs 5 DSG.
[67] *Pollirer/Weiss/Knyrim*, DSG² § 12 Anm 17.
[68] Siehe sogleich Punkt 1.2.2.
[69] Vgl § 12 Abs 5 DSG.
[70] § 12 Abs 3 Z 1 DSG.
[71] *Jahnel*, Handbuch Datenschutzrecht, Rz 4/144.
[72] § 12 Abs 3 Z 2 DSG.
[73] *Lehner* in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht, 125.
[74] *Jahnel*, Handbuch Datenschutzrecht, Rz 3/78.
[75] Vgl u.a. §§ 8 Abs 1 Z 2 und 9 Z 6 DSG.
[76] *Pollirer/Weiss/Knyrim*, DSG² § 12 Anm 12.

oder unmittelbar anwendbar sind,[77] damit Daten für private Zwecke oder publizistische Tätigkeiten übermittelt werden,[78] die Übermittlung für die Erfüllung eines zwischen Auftraggeber und Betroffenen bzw. einem Dritten eindeutig im Interesse des Betroffenen geschlossenen Vertrages notwendig ist,[79] die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden,[80] der Datentransfer in einer Standard- oder Musterverordnung ausdrücklich angeführt ist,[81] es sich um einen Datenverkehr mit österreichischen Dienststellen im Ausland handelt,[82] oder wenn die Übermittlung oder Unterlassung aus Datenanwendungen erfolgt, die gemäß § 17 Abs 3 DSG von der Meldepflicht ausgenommen sind.[83] Mit letzterer Bestimmung können Daten ziviler und militärischer Geheimdienste, sonstige militärische Daten oder sicherheitsbehördliche Daten, die der Verbrechensbekämpfung dienen, ohne Genehmigung der DSB – jedoch unter Beachtung des § 12 Abs 5 DSG – ins Ausland übermittelt oder überlassen werden.[84] Das bedeutet, dass auch in diesem Fall bei Übermittlungen die Vorschriften des § 7 DSG einzuhalten bzw bei Überlassungen eine schriftliche Zusage des empfangenden Dienstleisters, die Dienstleisterpflichten einzuhalten,[85] einzuholen ist.

Neben dieser taxativen Aufzählung öffnet § 12 Abs 4 DSG ein weiteres Feld für den genehmigungsfreien Datentransfer. Demnach ist eine Datenübermittlung oder -überlassung immer dann, wenn sie zur Wahrung eines wichtigen öffentlichen Interesses oder eines lebenswichtigen Interesses einer Person derart dringend notwendig ist, dass eine – ansonsten erforderliche – Genehmigung der DSB nicht eingeholt werden kann, auch ohne Genehmigung zulässig. Allerdings muss dieser Datentransfer umgehend der DSB mitgeteilt werden.[86]

b. Datentransfer in EU-Mitgliedsstaaten und EWR-Vertragsstaaten

In § 12 DSG wird gleich zu Beginn klargestellt, dass der Datentransfer jedenfalls an Empfänger in Mitgliedsstaaten der EU genehmigungsfrei ist. Seit der DSG-Novelle 2010 wurde dieser Empfängerkreis auf Norwegen, Island und Liechtenstein, sohin auf den

[77] § 12 Abs 3 Z 3 DSG.
[78] § 12 Abs 3 Z 4 DSG.
[79] § 12 Abs 3 Z 6 DSG.
[80] § 12 Abs 3 Z 7 DSG.
[81] § 12 Abs 3 Z 8 DSG.
[82] § 12 Abs 3 Z 9 DSG.
[83] § 12 Abs 3 Z 10 DSG.
[84] *Pollirer/Weiss/Knyrim*, DSG² § 12 Anm 15.
[85] Siehe oben 1.4.1.b
[86] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/154.

gesamten EWR-Raum ausgeweitet. Dem zu Grunde liegen die im EWR-Abkommen enthaltene Übernahme der DSRL und die vielfachen Überlegungen, dieses sei ohnehin unmittelbar anwendbar. Begründet wurde dies durch die ständige Rechtsprechung des EuGH, wonach Bestimmungen von Assoziationsabkommen (das EWR-Abkommen ist ein solches) einen integrierenden Bestandteil des Gemeinschaftsrechts bilden würden.[87] Die dafür notwendige Klarheit und Unbedingtheit der jeweiligen Bestimmung sei im Fall der Übernahme der DSRL gegeben, zumal eindeutig erkennbar sei, dass die DSRL auch zwischen den EWR-Vertragsstaaten gelten soll.[88]

Diesem Umstand wurde nun auch durch die ausdrückliche Bezugnahme auf den EWR-Vertragsraum in § 12 DSG Rechnung getragen. Übermittlungen und Überlassungen von Daten in Vertragsstaaten des EWR sind daher jedenfalls genehmigungsfrei.[89]

c. Drittstaaten mit angemessenen Datenschutzniveau

Ebenfalls keiner Genehmigung der DSB bedarf der Datentransfer in Drittstaaten, die ein angemessenes Datenschutzniveau aufweisen.[90] Für die Beurteilung, wann ein angemessenes Datenschutzniveau vorliegt und wie ein solches zu qualifizieren ist, sind gemäß Artikel 25 DSRL alle Umstände zu berücksichtigen, die bei einer Datenübermittlung eine Rolle spielen. Insbesondere sind die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden Rechtsnormen zu berücksichtigen.[91]

Die Europäische Kommission kann in einem Verfahren nach Artikel 31 Abs 2 DSRL feststellen, wann ein Drittland ein angemessenes Datenschutzniveau festlegt. Leitlinien[92] für die Bewertung des Vorliegens eines gleichwertigen Schutzniveaus wurden von der Datenschutzgruppe, die aufgrund von Artikel 29 der DSRL eingesetzt wurde, erstellt.[93]

In Österreich obliegt die Feststellung, welche Drittstaaten ein angemessenes Datenschutzniveau gewährleisten, dem Bundeskanzler, der dies mittels Verordnung

---

[87] Seit EuGH 30.09.1987, Rs 12/86 (Demirel).
[88] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/136.
[89] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/136.
[90] § 13 Abs 2 DSG.
[91] Vgl Art 25 Abs 2 DSRL.
[92] Vgl *Artikel-29-Datenschutzgruppe:* Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, GD XV D/5025/98, WP 12 <ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf> (24.08.2014).
[93] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/137.

kundzutun hat.[94] Zudem sind auch die Feststellungen, die die Europäische Kommission in den Verfahren nach Artikel 31 Abs 2 DSRL zum Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus getroffen hat, per Verordnung zu veröffentlichen.[95] In der aufgrund dieser Ermächtigung erlassenen Verordnung über den angemessenen Datenschutz in Drittstaaten (im Folgenden kurz *„DSAV“*) [96] sind aktuell jene Drittländer gelistet, welchen ein angemessenes Datenschutzniveau zugebilligt wird. Für jene neun Länder, die in § 1 DSAV aufgezählt sind (Schweiz, Argentinien, Guernsey, Insel Man, Jersey, Färöer Inseln, Andorra, Uruguay und Neuseeland) gilt dies ohne Einschränkung. Der Großteil dieser Länder wurde jedoch nicht auf Basis nationaler Adäquanzentscheidungen, sondern aufgrund von entsprechenden Entscheidungen der Europäischen Kommission in diese Liste aufgenommen.

In § 2 DSAV hingegen wird die Genehmigungsfreiheit von Überlassungen und Übermittlungen in bestimmte Drittländer jeweils an die Einhaltung weiterer Voraussetzungen geknüpft. Der wichtigste Fall hierbei ist der Datentransfer in die Vereinigten Staaten von Amerika.[97] Dieser ist dann genehmigungsfrei, wenn er an Empfänger gerichtet ist, die dem sogenannten Safe-Harbor-System beigetreten sind. Mit einem solchen Beitritt verpflichten sich die Unternehmen, die Safe Harbor Principles und die dazugehörenden verbindlichen Frequently Asked Questions zu beachten.[98] Die Europäische Kommission hat am 26.07.2000 entschieden, dass bei einem Datentransfer an ein solches Safe-Harbor-Unternehmen ein ausreichendes Datenschutzniveau gewährleistet ist.[99] Diese Entscheidung wurde von der Kommission einseitig gefällt – weswegen die landläufig verbreitete Bezeichnung *„Safe-Harbour-Abkommen“* irritierend ist – und steht derzeit vor einer umfangreichen Evaluierung. Auch auf Druck des Europäischen Parlamentes forderte die Kommission die Vereinigten Staaten zur Stellungnahme und Nachbesserung in 13 Punkten auf. Im Zeitpunkt der Finalisierung der gegenständlichen Arbeit lag der Europäischen Kommission noch keine vollständige Antwort der Vereinigten Staaten vor. Diese wird für Herbst 2014 erwartet und könnte gegebenenfalls noch im Laufe des Jahres 2014 die Safe-Harbour-Erklärung seitens der Europäischen Kommission widerrufen werden. Tritt dies ein, würde fortan ein Datentransfer

---

[94] § 12 Abs 2 DSG.
[95] § 55 Z 1 DSG.
[96] Datenschutzangemessenheits-Verordnung, BGBl II 521/1999 idF BGBl II 213/2013.
[97] § 2 Abs 2 Z 1 DSAV.
[98] *Jahnel*, Handbuch Datenschutzrecht, Rz 4/140.
[99] Entscheidung der Europäischen Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EC.

in die Vereinigten Staaten jedenfalls einer Genehmigung durch die Aufsichtsbehörden – im Falle Österreichs der DSB – bedürfen.

Für den Bereich von Fluggastdaten wurde neben Safe-Harbor von der Europäischen Kommission eine weitere Adäquanzentscheidung getroffen. Seit der Unterzeichnung des PNR-Abkommens [100] im Juli 2007 ist die Übermittlung von Fluggastdatensätzen an das Ministerium für Innere Sicherheit der Vereinigten Staaten genehmigungsfrei zulässig.

Auch der genehmigungsfreie Datentransfer nach Kanada und Israel ist an das Vorliegen zusätzlicher – in § 2 DSAV genannter – Voraussetzungen gebunden.

1.4.3. Genehmigungspflichtiger Datenverkehr

a. Allgemeines

Liegt kein nach § 12 DSG genehmigungsfreier Datentransfer vor, ist vor der Übermittlung oder Überlassung eine Genehmigung der Datenschutzbehörde einzuholen.[101]

Diese darf die Genehmigung nur dann erteilen, wenn jedenfalls die oben genannten Grundvoraussetzungen [102] erfüllt sind. Die Übermittlung von Daten muss daher schon grundsätzlich gemäß §§ 7 ff DSG zulässig sein; bei einer Überlassung müssen die Voraussetzungen der §§ 10 f gegeben sein. Denkbar und zulässig ist die Erteilung der Genehmigung unter der Voraussetzung der Erfüllung von Bedingungen und Auflagen.[103]

b. Besondere Voraussetzungen

Neben diesen Grundvoraussetzungen muss die DSB für die Erteilung einer Genehmigung im Rahmen ihrer Prüfung auch zum Ergebnis kommen, dass für den zu genehmigenden Datentransfer im Einzelfall das Bestehen eines angemessenen Datenschutzniveaus glaubhaft gemacht wurde.[104] Dies ist etwa dann gegeben, wenn im Empfängerstaat zwar nicht in seiner Gesamtheit, jedoch für einzelne Bereiche ein angemessenes Datenschutzniveau besteht.[105] Die Prüfung hat dabei wieder anhand der oben erwähnten allgemeinen Bestimmungen,

---

[100] Abkommen zwischen der Europäischen Kommission und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS), ABl L 2007/204, 18.
[101] § 13 Abs 1 DSG.
[102] Siehe oben 1.4.1.
[103] § 13 Abs 1, letzter Satz DSG.
[104] § 13 Abs 2 Z 1 DSG.
[105] *Jahnel*, Handbuch Datenschutzrecht, Rz 4/158.

insbesondere der Art der verwendeten Daten, der Zweckbestimmung sowie der Dauer der geplanten Verwendung, den beteiligten Ländern und ihrer Rechtsnormen zu erfolgen. [106]

Sollte nicht einmal für einzelne Bereiche ein angemessener Datenschutz im Empfängerstaat vorliegen, kann der Datentransfer unter folgender Voraussetzung dennoch genehmigt werden: Macht der Auftraggeber glaubhaft, dass die schutzwürdigen Interessen des Betroffenen auch im Ausland ausreichend gewahrt werden, ist die Genehmigung – bei Vorliegen der sonstigen, allgemeinen Voraussetzungen – zu erteilen. [107] Die im Gesetz ausdrücklich erwähnte Möglichkeit, diese Glaubhaftmachung über vertragliche Zusicherungen des Empfängers zu erreichen, ist auch das gängigste Mittel zur Verwirklichung dieser – als Auffangtatbestand konzipierten – Bestimmung.[108]

c. Vertragliche Zusicherung – Standardvertragsklauseln

Das zentrale Instrument im Zusammenhang mit der Glaubhaftmachung über vertragliche Zusicherungen stellen die sogenannten Standardvertragsklauseln der EU dar. Dabei handelt es sich um an die Mitgliedsstaaten gerichtete Vorschläge der Europäischen Kommission, wie Vertragswerke ausgestaltet werden sollten, damit dadurch ein angemessenes Schutzniveau[109] und die Möglichkeit der Durchsetzung sowohl für die Vertragsparteien als auch für den Betroffenen [110] gewährleistet sind. Die Standardvertragsklauseln stehen derzeit für Datenübermittlungen in zwei Versionen [111] und in einer zusätzlichen Version [112] für das Überlassen von Daten an Dienstleister zur Verfügung. Werden diese Standardvertragsklauseln unverändert verwendet, ist die DSB verpflichtet, diese als ausreichende Garantien für das Bestehen eines angemessenen Datenschutzniveaus anzuerkennen.[113] Werden Veränderungen vorgenommen, hat die DSB im Einzelfall zu überprüfen, ob trotz dieser Veränderungen die vertragliche Vereinbarung den Nachweis eines angemessenen Schutzniveaus erbringt. Selbst wenn dieser Nachweis durch Abschluss einer Standardvertragsklausel als erbracht anzusehen

---

[106] Siehe oben 1.4.2.c.
[107] § 13 Abs 2 Z 1 DSG.
[108] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/159.
[109] ErwGr 1 Entscheidung der Kommission vom 15.06.2001 (2001/497/EG).
[110] ErwGr 16 Entscheidung der Kommission vom 15.06.2001 (2001/497/EG).
[111] Entscheidung der Kommission vom 15.06.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, 2001/497/EG („Standardvertrag I“) und Entscheidung der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2001/475/EG bezüglich der Einführung alternativer Standardvertragsklauseln, 2004/915/EG („Standardvertrag II“).
[112] Beschluss der Kommission vom 05.02.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer nach der Richtlinie 95/46/EG, 2010/87/EU.
[113] ErwGr 6 Entscheidung der Kommission vom 15.06.2001 (2001/497/EG).

sein sollte, entfällt nach der Spruchpraxis[114] der DSB (im Entscheidungszeitpunkt noch als Datenschutzkommission) keinesfalls die Genehmigungspflicht.[115] Die DSB muss sohin dennoch die Genehmigung erteilen. Aufgrund des dann allerdings bereits erbrachten Nachweises des angemessenen Datenschutzniveaus wird diese Hürde in der Regel jedoch kein Problem darstellen.

d. Einseitige Zusage – Binding Corporate Rules

Seit der DSG-Novelle 2010 steht demjenigen, der um Genehmigung ansucht, neben einer zweiseitigen vertraglichen Vereinbarung auch die Möglichkeit offen, durch eine einseitige Zusage glaubhaft zu machen, dass die Interessen des Betroffenen nicht beeinträchtigt werden. Diese Zusagen werden durch die Registrierung bei der DSB verbindlich.[116]

Damit wird vor allem auf die Anforderungen der Wirtschaft abgestellt, zumal eine zwei konzernverbundenen Unternehmen auferlegte Verpflichtung, eine vertragliche Vereinbarung miteinander abzuschließen, nicht zielführend sein würde. Daher können Konzernmuttergesellschaften für Datenübermittlungen im Konzern durch die Zusage, im Konzern für alle datenempfangenden Töchter verbindliche unternehmensinterne Vorschriften über die Datenverarbeitung – sog Binding Corporate Rules – einzuführen, ein angemessenes Datenschutzniveau glaubhaft machen.[117] Diese Möglichkeit nutzen vor allem multinationale Konzerne mit Standorten in Ländern, die kein angemessenes Datenschutzniveau aufweisen. Im Unterschied zu den Standardvertragsklauseln existiert keine Musterformulierung und sind die BCR je Unternehmen neu auszuarbeiten und anschließend daran von der zuständigen nationalen Datenschutzbehörde zu genehmigen.

e. Konzerninterner Datentransfer als Standardanwendung

Wie bereits oben[118] dargestellt, ist auch jeder Datentransfer genehmigungsfrei, wenn er in einer Standard- oder Musterverordnung ausdrücklich angeführt ist.[119] Drei von den in der Standard- und Musterverordnung 2004[120] angeführten Standardanwendungen könnten dabei

[114] U.a. DSK 05.12.2008, K178.274/0010-DSK/2008.
[115] *Jahnel*, Handbuch Datenschutzrecht, Rz 4/160.
[116] § 13 Abs 2 Z 2 DSG.
[117] *Pollirer/Weiss/Knyrim*, DSG² § 13 Anm 8.
[118] Siehe oben 1.4.2.a
[119] § 12 Abs 3 Z 8 DSG.
[120] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004), StF: BGBl II 312/2004 idF BGBl II 514/2013.

auf den ersten Blick möglicherweise den Weg zur Genehmigungsfreiheit von Datentransfers innerhalb eines Konzerns ebnen.

Entgegen ihrem Wortlaut jedoch postuliert die Standardanwendung SA033 (*„Datenübermittlung im Konzern“*) kein generelles Privileg für Konzerne, personenbezogene Daten zwischen den verbundenen Unternehmen und über Staatsgrenzen hinweg zu übermitteln. Von der Standardanwendung sind lediglich Daten in Kontakt- und Termindatenbanken, Karrieredatenbanken und Bonus- und Beteiligungsprogrammen umfasst.[121]

Im Rahmen der Standardanwendung SA001 *(„Rechnungswesen und Logistik“*) können lediglich Kundendaten bei Lieferanten an die Konzernleitung des Auftraggebers mit Sitz in Drittstaaten genehmigungsfrei übermittelt werden, nicht jedoch Daten nichtgewerblicher Kunden, vor allem von Konsumenten. Ebenso wenig ist eine Weitergabe von Kundendaten an Gesellschaften desselben Konzerns oder zu Marketingzwecken an Unternehmen außerhalb des EWR ohne Genehmigung zulässig. [122] Auch für Personaldaten steht über Standardanwendungen – zu denken wäre an SA002 (Personalverwaltung für privatrechtliche Dienstverhältnisse) – kein Weg zu einer Genehmigungsfreiheit für eine Übermittlung innerhalb eines Konzerns offen.[123]

f. Sanktionen

Das Sanktionssystem der derzeitigen Rechtslage knüpft an das Vorliegen einer Genehmigung an. Der Datentransfer ins Ausland ohne Einholung einer erforderlichen Genehmigung der DSB stellt gemäß § 52 Abs 2 Z 2 DSG eine Verwaltungsübertretung dar und ist – seit der Erhöhung durch die DSG-Novelle 2010 – mit einer Verwaltungsstrafe von bis zu € 10.000,00 bedroht. Bereits daraus wird ersichtlich, dass derzeit vor allem in Fällen, in denen multinationale Konzerne als Auftraggeber Verstöße begehen, das Sanktionssystem aufgrund der Unverhältnismäßigkeit des dort zumeist gegebenen Jahresumsatz zur im Vergleich geringen Strafdrohung als zahnlos bezeichnet werden muss.

---

[121] *Waidmann*, Konzerninterner Austausch personenbezogener Daten, ecolex 2014, 7.
[122] *Waidmann*, ecolex 2014, 7.
[123] *Waidmann*, ecolex 2014, 7.

2. Die Rechtslage nach der Datenschutz-Grundverordnung

Der Entwurf zur Reform des europäischen Datenschutzrechtes der Europäischen Union ist zweigeteilt. Neben einem allgemeinen Datenschutzrecht, dessen Regelungen in Verordnungsform gegossen sind, soll das spezielle Datenschutzrecht im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in einem eigenen Regelungswerk normiert werden.[124] Dieses besondere Datenschutzrecht soll – anstatt des bisherigen Rahmenbeschlusses[125] – in Form einer Richtlinie[126] erlassen werden. Inhalt der gegenständlichen Untersuchung ist jedoch ausschließlich der Datentransfer ins Ausland im Bereich des allgemeinen Datenschutzrechtes. Diese Regelungen finden Niederschlag in der geplanten Datenschutz-Grundverordnung (*„DS-GVO"*).

Die DS-GVO ist noch nicht in Kraft getreten ist, sodass auch der finale Text und die finalen Formulierungen noch nicht feststehen. Für die weiteren Ausführungen bildet daher der am 21.11.2013 vom Ausschuss des Europäischen Parlamentes für bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingereichte Entwurf für die Europäische Datenschutz-Grundverordnung, der am 12.03.2014 von den Abgeordneten des Europäischen Parlamentes akzeptiert wurde. Die gegenständlich relevanten und in der Arbeit bearbeiteten Regelungen sind in dieser Fassung im Anhang beigeschlossen.

Im Gegensatz zum ersten Kapitel, der Beleuchtung der aktuellen Rechtslage, wird im Nachfolgenden nicht mehr das Begriffspaar *„Auftraggeber"* und *„Dienstleister"* verwendet, zumal sich diese auch nicht in der DS-GVO finden. Für deren Analyse wird – nachdem eine nationale Um- und Übersetzung nicht zu erwarten ist – auf die dort verwendeten Begriffe des *„für die Verarbeitung Verantwortlichen"* (= Auftraggeber iSd DSG) und des *„Auftragsverarbeiters"* (= Dienstleister iSd DSG) abgestellt.

2.1. Anzuwendendes Recht

Verordnungen der EU sind laut Vertrag über die Arbeitsweise der Europäischen Union allgemein und unmittelbar geltende und in allen ihren Teilen verbindliche Rechtsakte.[127] Aufgrund dieser Durchgriffswirkung müssen sie von den Mitgliedsstaaten nicht in nationales

[124] Vgl *Lachmayer*, Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, ÖJZ 2012/92, 841.
[125] Rahmenbeschluss 2008/977/JI des Rates der Europäischen Union vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.
[126] Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg.
[127] Art 288 Abs 2 AEUV.

Recht umgesetzt werden. Es besteht vielmehr ein Verbot solcher Umsetzungen für den in der Verordnung geregelten Bereich, das auch Modifikationen dieser Regelungen grundsätzlich untersagt. Die EU-Bürger können aus der Verordnung direkt Ansprüche herleiten und ist die Verordnung Vorgabe für die nationalen Behörden und Gerichte in den Mitgliedsstaaten.[128] Ebenfalls ist für Auslegungsfragen der nationalen Gerichte einzig der EuGH nach den Regeln des Vorabentscheidungsverfahrens zuständig.[129]

Der Schutz personenbezogener Daten wird durch die unmittelbare Anwendung der Verordnung einheitlich geregelt. Aus diesem Grund erübrigt sich nach Inkrafttreten der DS-GVO die Frage nach der anzuwendenden nationalen Rechtsordnung. Vielmehr führt die Ausgestaltung des Regelungswerkes als Verordnung unweigerlich zur Frage, ob nach Inkrafttreten der DS-GVO die bisherigen nationalen Umsetzungsgesetze der DSRL – in Österreich das DSG – überflüssig werden. Für jene Bereiche, die unionsrechtlich durch die DS-GVO geregelt sind, muss die Frage bejaht werden. Nicht darunter fällt beispielsweise der Schutz von Daten juristischer Personen, der bisher ebenfalls durch das DSG gewährt wird.[130] Auch Konkretisierungen der Verordnung durch die nationalen Gesetzgeber sind nach Inkrafttreten denkbar. Vereinzelt finden sich in der DS-GVO entsprechende Ermächtigungen, *„im Einklang mit den Regelungen dieser Verordnung“*[131] die Vorgaben der DS-GVO durch nationale Rechtsvorschriften zu konkretisieren.[132]

Entschließt sich der österreichische Gesetzgeber, den Datenschutz für juristische Personen weiterhin aufrecht zu halten, wird es weiterhin ein eigenes österreichisches Datenschutzgesetz geben. Sollte dies nicht der Fall sein und gleichzeitig Überlegungen angestellt werden, die einzelnen Konkretisierungen in die jeweiligen Materiengesetzen[133] einzuarbeiten, ist ein Außerkrafttreten des österreichischen Datenschutzgesetzes denkbar. Aller Voraussicht nach ist jedoch mit einer Aufrechterhaltung des DSG selbst bei Fallenlassen des Schutzes von Daten juristischer Personen zu rechnen, zumal sich die politische Bereitschaft, nationale Gesetze gänzlich durch EU-Verordnungen zu ersetzen, in Grenzen halten wird. Zudem dürften die in der DS-GVO enthaltenen Regelungsermächtigungen für die nationalen Gesetzgeber ausreichend Substrat für ein (weiterhin vorhandenes) Datenschutzgesetz liefern.

---

[128] *Gola*, Handbuch Datenschutz[23] (2014), 327.
[129] Art 267 Abs 2 lit b AEUV.
[130] Siehe sogleich Punkt 2.2.
[131] So wörtlich Artikel 82 Abs 1 DS-GVO.
[132] Etwa Artikel 82 Abs 1 DS-GVO für die Verarbeitung personenbezogener Arbeitnehmerdaten; Art 80 Abs 1 Z 1 hinsichtlich Datenverarbeitung zu journalistischen Zwecken.
[133] ZB ArbVG.

Jedenfalls aber werden mit dem Inkrafttreten der DS-GVO nationale Kollisionsregeln über das anwendbare Recht nicht mehr benötigt.[134] Lediglich für den Fall der Aufrechterhaltung des Datenschutzes juristischer Personen wird der Gesetzgeber entsprechende Regelungen zu treffen haben.

Der räumliche Anwendungsbereich der DS-GVO umfasst alle Datenverarbeitungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern mit einer Niederlassung in einem Mitgliedsstaat der EU, sofern diese Verarbeitung im Rahmen der Tätigkeiten dieser Niederlassung durchgeführt wird. Wo diese Verarbeitung durchgeführt wird, insbesondere dass sie innerhalb der Union durchgeführt werden müsse, ist durch die Klarstellung im Entwurf des LIBE-Ausschusses für die Anwendbarkeit der Verordnung nicht mehr relevant.[135] Somit ist auch der Schutz der Daten umfasst, die von für die Verarbeitung Verantwortliche oder Auftragsverarbeiter in Drittstaaten verarbeiten (lassen), unabhängig davon, ob es sich dabei um Daten von in der Union ansässigen betroffenen Personen handelt.

Lediglich bei für die Verarbeitung Verantwortlichen aus Drittstaaten wird nach der Herkunft des Betroffenen differenziert: Personen, die innerhalb der Union ansässig sind, erfahren hinsichtlich des Schutzes ihrer personenbezogenen Daten eine bevorzugte Behandlung gegenüber nicht in der Union ansässigen Betroffenen, weil unter bestimmten Voraussetzungen auch Datenverarbeitungen von für die Verarbeitung Verantwortlichen, die nicht in der Union ansässig sind, ebenfalls unter den Schutzbereich der DS-GVO fallen.[136]

Der erste Tatbestand, der diese Folge nach sich zieht, sind Datenverarbeitungen, die dazu dienen, den betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten.[137] Die nunmehrige Fassung der DS-GVO stellt – im Unterschied zum Kommissionsvorschlag – eindeutig nicht mehr darauf ab, ob als Gegenleistung für die angebotenen Waren oder Dienstleistungen eine Zahlung zu erfolgen hat. Daher erstreckt sich der Schutzbereich der DS-GVO auch auf schenkungsweise angebotene Waren und Dienstleistungen sowie solche, bei denen eine Zahlung aus (anderen) rechtlichen Gründen nicht getätigt werden muss.

Als zweiter Fall sollen auch Datenverarbeitungen von für die Verarbeitung Verantwortlichen aus Drittstaaten, die auf die Überwachung der betroffenen Personen abzielen, vom Schutzbereich der DS-GVO umfasst sein. [138] Artikel 3 Abs 2 lit b des

[134] *Lachmayer*, ÖJZ 2012/92, 842.
[135] Art 3 Abs 1 DS-GVO.
[136] Art 3 Abs 2 DS-GVO.
[137] Art 3 Abs 2 lit a DSG.
[138] Art 3 Abs 2 lit b DSG.

Kommissionsvorschlages stellte noch auf eine *„Beobachtung“* des Verhaltens der betroffenen Person durch den Datenverarbeiter ab. Im Entwurf des LIBE-Ausschusses wurde dies insofern geändert und verschärft, als bereits ein *„Überwachen“* der betroffenen Person den Schutz der DS-GVO auslösen soll. Dadurch werden nicht nur Fälle umfasst, in denen die Internetaktivitäten der betroffenen Person mit Hilfe von Datenverarbeitungstätigkeiten beobachtet oder nachvollzogen werden,[139] sondern bereits alle Sachverhalte, bei denen Daten über Personen mit Hilfe von Datenverarbeitungstätigkeiten erhoben oder verfolgt werden.[140] Bereits die mitunter zeitgleiche Verfolgung und nicht erst die Nachvollziehung im Nachhinein ist daher umfasst.

Durch die beiden obigen Fallkonstellationen sollen für die Verarbeitung Verantwortliche aus Drittstaaten, die ihre Tätigkeiten auf Mitgliedstaaten der EU ausrichten, verpflichtet werden, das europäische Datenschutzniveau einzuhalten. Trotz dieser Ausweitung ist in Summe eine Einschränkung des räumlichen Anwendungsbereiches der DS-GVO insofern zu erkennen, als für die Verarbeitung Verantwortliche und Auftragsverarbeiter, die nicht in der EU niedergelassen sind, nur in jenen beiden erwähnten – in Artikel 3 Abs 2 gelisteten – Fällen unter die Anwendung der DS-GVO fallen. Dadurch fällt im Gegensatz zur bisherigen Regelung der DSRL [141] etwa die bloße Nutzung von in der Union gelegenen Verarbeitungsmitteln durch für die Verarbeitung Verantwortliche aus Drittstaaten nicht unter die DS-GVO, selbst wenn Daten von in der EU ansässigen betroffenen Personen verarbeitet werden.[142]

Die Differenzierung bei für die Verarbeitung Verantwortlichen und Auftragsverarbeitern aus Drittstaaten nach dem Zweck der Datenverarbeitung erscheint – bei allen zu erwartenden Nachweisschwierigkeiten – sinnvoll und adäquat. Eine ähnliche Lösung wurde bereits von der Artikel-29-Datenschutzgruppe vorgeschlagen.[143] Damit lässt sich einerseits verhindern, dass internationale Unternehmen aus Drittstaaten bloß wegen der Furcht aus einem Mitgliedsstaat abwandern, dem EU-Datenschutzrecht zu unterliegen, selbst wenn sie ihren Geschäftsbetrieb nicht auf einen EU-Mitgliedsstaat ausgerichtet haben. Andererseits bleibt mit dieser Lösung das Hauptproblem, nämlich das (unzulässige) Verarbeiten von Daten europäischer Internetbenutzer vom Schutzbereich umfasst. Zudem können sich nun etwa Betreiber von

---

[139] ErwGr 21 KOM (2012) 11 endg.
[140] ErwGr 21 DS-GVO, Fassung Entwurf des LIBE-Ausschusses.
[141] Siehe oben 1.1.
[142] *Dörnhöfer* in Jahnel, Datenschutzrecht und E-Government, Jahrbuch 2012, 70.
[143] *Artikel-29-Datenschutzgruppe:* Stellungnahme 8/2010 zum anwendbaren Recht vom 16.12.2010, 0836-02/10/DE, WP 179, 30 <http://www.cnpd.public.lu/de/publications/groupe-art29/wp179_de.pdf> (24.08.2014).

Onlinediensten nicht mehr darauf berufen, dass für sie ohne Niederlassung in der EU das europäische Datenschutzrecht nicht gelte.[144]

2.2. Sachlicher Anwendungsbereich

Wie schon bereits die Datenschutzrichtlinie, umfasst auch die DS-GVO nur den Schutz von Daten natürlicher Personen, nicht jedoch von juristischen Personen.[145] Zum einen lautet der Untertitel der DS-GVO gleich wie jener der DSRL (*„zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“*) und zum anderen wird – in erneut konsequenter Weise – die Definition der personenbezogenen Daten an jene der betroffenen Person geknüpft und als solche (lediglich) *„eine bestimmte oder bestimmbare natürliche Person“*[146] angesehen.

Die Daten juristischer Personen sind demnach ausdrücklich nicht vom Schutzbereich der DS-GVO umfasst, obwohl dies beispielsweise innerhalb des Europäischen Parlaments vom Ausschuss für Industrie, Forschung und Energie vorgeschlagen wurde. Diesbezüglich ist auch – insbesondere aufgrund des auf europäischer Ebene jahrzehntelangen Fokus ausschließlich auf den Schutz natürlicher Personen sowie der ausdrücklichen Erwähnung im Untertitel – bis zum Inkrafttreten keine Änderung zu erwarten.

2.3. Datentransfer ins EU-Ausland

2.3.1. Ausgangslage

Die DSRL ist als Richtlinie zwar nicht in den einzelnen Mitgliedsstaaten direkt anwendbar, führt bisher dennoch über weite Teile des Datenschutzrechtes insofern zu einer Harmonisierung, als sie bei Umsetzungsmängel entweder direkt anzuwenden ist oder in diesen Fällen die nationalen Umsetzungsgesetze richtlinienkonform zu interpretieren sind. Trotzdem war und ist ein einheitliches Datenschutzniveau innerhalb der Mitgliedsstaaten derzeit nicht gegeben. Die dadurch entstehenden Probleme können die Mitgliedsstaaten nach Ansicht der EU nicht selbst überwinden, weshalb – um einen reibungslosen Transfer personenbezogener Daten innerhalb der EU zu ermöglichen – Bedarf an einer harmonisierten und kohärenten Regelung besteht.[147] Vor diesem Hintergrund soll gleichzeitig aufgrund der

[144] *Schaar*, Europäischer Startschuss für die Datenschutzreform: Eine Chance für wirksame Verbesserungen, DuD 2012, 154.
[145] *Dörnhöfer* in Jahnel, Datenschutzrecht und E-Government, Jahrbuch 2012, 59.
[146] Art 4 Abs 2 DS-GVO.
[147] KOM (2012) 11 endg., 6.

technischen Veränderung von Wirtschaft und gesellschaftlichem Leben der Datentransfer innerhalb der EU sowie auch die Datenübermittlung an Drittländer noch weiter erleichtert, gleichzeitig aber einem hohen Maß an Datenschutz unterstellt werden.[148]

2.3.2. Übermittlung – Überlassung

Die im DSG derzeit enthaltene Sonderbehandlung des Überlassens von Daten im Vergleich zur Übermittlung fußt auf den unterschiedlichen Legaldefinitionen in § 4 DSG. Für die Übermittlung werden in § 7 DSG – insbesondere in dessen Abs 2 – spezielle Zulässigkeitsvoraussetzungen vorgesehen. Diese Bestimmung findet sich in dieser Form zwar nicht in der DSRL, ist jedoch als Umsetzung der Artikel 5 und 6 DSRL anzusehen. Die DSRL unterscheidet nicht zwischen Übermittlung und Überlassung, sondern subsummiert die Weitergabe durch Übermittlung bereits unter den allgemeinen Verarbeitungsbegriff.[149]

Diese Ausgestaltung findet sich nun auch in Artikel 4 Abs 3 DS-GVO wieder, der die *„Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung“* ganz allgemein als Verarbeitung einstuft, ohne dabei hinsichtlich des Empfängers zu differenzieren. Als *„Empfänger“* werden natürliche oder juristische Personen definiert, an welche Daten weitergegeben werden.[150] Im Unterschied zur im LIBE-Entwurf enthaltenen Definition eines *„Dritten“*[151] können auch Auftragsverarbeiter als Empfänger fungieren, was in Zusammenschau der Definitionen bedeutet, dass Datenweitergaben an Auftragsverarbeiter unter den Begriff der allgemeinen Datenverarbeitung fallen. Wie bereits in der DSRL wird daher in der DS-GVO keine Unterscheidung zwischen Übermitteln und Überlassen getroffen. Die Datenübertragung, die die derzeitige österreichische Lösung als Überlassen von Daten kennt, muss daher im Sinne der DS-GVO als Übermittlung von Daten qualifiziert werden. Diese Weitergabe an Auftragsverarbeiter wird jedoch – gemeint ist die Weitergabe selbst – jedenfalls für den Bereich der nicht-sensiblen Daten in aller Regel durch die positive Interessensabwägung zugunsten des für die Verarbeitung Verantwortlichen sowie den zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter abzuschließenden Vertrag gerechtfertigt sein.[152]

---

[148] ErwGr 6 DS-GVO.
[149] Art 2 lit b DSRL.
[150] Art 4 Abs 7 DS-GVO.
[151] Art 4 Abs 7a DS-GVO.
[152] Art 26 Abs 2 DS-GVO.

In weiterer Folge wird der Begriff der Überlassung mangels Niederschlag in der DS-GVO nicht mehr verwendet und jede Weitergabe von Daten an andere Personen als die betroffene Person generell als *„Übermittlung“* bezeichnet.

2.3.3. Übermittlung von nicht-sensiblen Daten[153]

Die Rechtmäßigkeit einer Verarbeitung – und damit auch einer Übermittlung – von personenbezogenen Daten, die nicht unter die Definition des Artikel 9 DS-GVO fallen, richtet sich nach Artikel 6 DS-GVO.

Auf den ersten Blick sind darin nicht allzu viele Veränderungen im Vergleich zur bisherigen Rechtslage ersichtlich. Einerseits, weil die unabhängig von der Art der Daten einzuhaltenden Grundsätze des Art 5 DS-GVO an jene des Art 6 DSRL angelehnt sind und andererseits, weil der bisherige Artikel 7 DSRL und der nunmehrige Artikel 6 DS-GVO beinahe ident abgefasst sind. In beiden finden sich folgende sechs Tatbestände, bei deren Verwirklichung die Verarbeitung/Übermittlung rechtmäßig erfolgt:

- Die Einwilligung der betroffenen Person.[154]
  Die Einzelheiten der Einwilligung – insbesondere die Beweispflicht des für die Verarbeitung Verantwortlichen, Widerrufsmöglichkeit und Zweckgebundenheit – werden erstmals in einem eigenen Artikel zusammengefasst.[155]
- Die Verarbeitung ist zur Erfüllung eines Vertragsverhältnisses notwendig, dessen Vertragspartei die betroffene Person ist.[156]
- Die Verarbeitung ist zur Erfüllung einer gesetzlichen Pflicht des für die Verarbeitung Verantwortlichen notwendig.[157]
- Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person notwendig.[158]
- Die Verarbeitung ist zur Wahrnehmung einer Aufgabe im öffentlichen Interesse notwendig.[159]

---

[153] Art 9 Abs 1 DS-GVO definiert wie schon Art 8 DSRL sensible Daten als besondere Datenkategorie. Darunter sind Daten zu verstehen, aus denen die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, sexuelle Orientierung oder Geschlechtsidentität oder die Mitgliedschaft und Betätigung in einer Gewerkschaft hervorgehen sowie genetische (Art 4 Abs 10 DS-GVO) oder biometrische (Art 4 Abs 22 DS-GVO) Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten oder mutmaßliche Straftaten, Verurteilungen oder damit zusammenhängende Sicherungsmaßregeln.
[154] Art 7 lit a DSRL; Art 6 Abs 1 lit a DS-GVO.
[155] Art 7 DS-GVO.
[156] Art 7 lit b DSRL; Art 6 Abs 1 lit b DS-GVO.
[157] Art 7 lit c DSRL; Art 6 Abs 1 lit c DS-GVO.
[158] Art 7 lit d DSRL; Art 6 Abs 1 lit d DS-GVO.

- Die Verarbeitung ist zur Wahrung berechtigter Interessen des für die Verarbeitung Verantwortlichen oder – im Fall einer Weitergabe – des Dritten notwendig.[160] Überwiegen jedoch die Interessen oder die Grundfreiheiten und Grundrechte des Betroffenen, hat die Verarbeitung zu unterbleiben.

  Im Rahmen dieses Rechtfertigungsgrundes ist beachtlich, dass zwar bereits Artikel 7 DSRL den Fall der Weitergabe und damit die Interessen des Dritten beinhaltet, dieser jedoch im ersten veröffentlichten Kommissionsvorschlag der DS-GVO fehlte. Erst in der aktuellen Fassung wurde die Bestimmung durch den LIEBE-Ausschuss entsprechend ergänzt. Gleichzeitig wurde klargestellt, dass nicht irgendwelche berechtigte Interessen des für die Verarbeitung Verantwortlichen bzw des Dritten geschützt sein können, sondern lediglich jene, die die berechtigten Erwartungen der betroffenen Person erfüllen und von diesen aus ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen abgeleitet werden.

Im Unterschied zur DSRL legt die DS-GVO hingegen ausdrücklich fest, dass für Datenverarbeitungen, die nach Art 6 Abs 2 lit c (gesetzliche Verpflichtung) oder lit e (öffentliches Interesse) gerechtfertigt sein sollen, eine Rechtsgrundlage entweder im Unionsrecht oder im Recht des Mitgliedsstaates, dem der für die Verarbeitung Verantwortliche unterliegt, vorhanden sein muss.[161] Ist letzteres nicht möglich (etwa weil der für die Verarbeitung Verantwortliche seinen Sitz in einem Drittland hat), ist ausschließlich Unionsrecht heranzuziehen. Eine diesbezügliche Repräsentation durch den Dritten, insbesondere eine Heranziehung der Rechtsordnung, welcher ein – allenfalls empfangender – Dritter unterliegt, ist mangels entsprechender Erwähnung nicht zulässig.[162]

Unterschiede zur bisherigen (österreichischen) Rechtslage können sich nunmehr vor allem deswegen ergeben, weil die Divergenzen zwischen den Vorgaben der DSRL und der Umsetzung im DSG nunmehr wegfallen. An dieser Stelle soll aber nicht unerwähnt bleiben, dass diesen Divergenzen – unabhängig davon, ob sie im Verfassungsrang stehen oder im einfachgesetzlichen Teil des DSG enthalten sind – schon bisher nach Ansicht von *Jahnel* zumeist mit richtlinienkonformer Interpretation zu begegnen war.[163]

---

[159] Art 7 lit e DSRL; Art 6 Abs 1 lit e DS-GVO.
[160] Art 7 lit f DSRL; Art 6 Abs 1 lit f DS-GVO.
[161] Art 6 Abs 3 DS-GVO.
[162] Art 6 Abs 3 lit b DS-GVO.
[163] *Jahnel*, Handbuch Datenschutzrecht, u.a. Rz 1/41 f, 4/37, 4/39.

Artikel 6 Abs 3, wie er noch im ersten Kommissionsentwurf lautete, wurde in der aktuellen Fassung der DS-GVO um folgende Regelung ergänzt:

> *„Im Rahmen dieser Verordnung können im Recht der Mitgliedstaaten Einzelheiten der Rechtmäßigkeit der Verarbeitung, insbesondere zu den für die Verarbeitung Verantwortlichen, zur Zweckbestimmung der Verarbeitung und Zweckbindung, zur Art der Daten und zu den betroffenen Personen, zu Verarbeitungsvorgängen und -verfahren, zu Empfängern sowie zur Speicherdauer geregelt werden.“*[164]

Aufgrund der Positionierung dieser Ergänzung und deren Einbindung in Art 6 Abs 3 DS-GVO liegt die Vermutung nahe, dass sich diese Ermächtigung zur Konkretisierung durch die nationalen Gesetzgeber lediglich auf die von Art 6 Abs 3 geregelten Sachverhalte, sohin die Datenverarbeitungen gemäß Art 6 Abs 1 lit c (gesetzliche Verpflichtung) und lit e (öffentliches Interesse) DS-GVO erstreckt. Die dennoch offen gewählte Formulierung indiziert jedoch möglicherweise, dass diese Konkretisierungsmöglichkeit auch für alle anderen genannten Rechtfertigungsgründe offensteht.

Zur Klärung dieser Frage dient ein Blick auf die systematische Eingliederung. Wäre beabsichtigt gewesen, dem Gesetzgeber die Kompetenz, Einzelheiten selbst zu regeln, für alle Rechtfertigungsgründe zu erteilen, wäre eine Positionierung in Art 6 Abs 3 verfehlt. Ein Redaktionsversehen ist diesbezüglich ebenfalls nicht zu erkennen, zumal es leicht möglich gewesen wäre, einen neuen Absatz einzufügen. Den Mitgliedstaaten wird daher offensichtlich nicht allgemein, sondern nur in jenen Bereichen Regelungsbefugnis eingeräumt, in denen die Rechtfertigung der Datenverarbeitung auf ihren Rechtsakten basieren kann.[165]

Das führt im Umkehrschluss und in Zusammenschau mit der unmittelbaren Geltung der Verordnung dazu, dass – jedenfalls im Bereich der anderen Rechtfertigungsgründe – keine generelle Möglichkeit für die Mitgliedstaaten besteht, Einzelheiten der Rechtmäßigkeit der Verarbeitung national zu konkretisieren. Daraus kann insbesondere abgeleitet werden, dass die oben zitierte eingeführte Regelung keine Ermächtigung für den österreichischen Gesetzgeber normiert, wiederum nach dem Empfänger der transferierten Daten zu differenzieren, sohin eine Unterscheidung zwischen Übermittlung und Überlassung von Daten vorzusehen.

---

[164] Art 6 Abs 3 letzter Satz DS-GVO.
[165] Art 6 Abs 1 lit c und e DS-GVO.

2.3.4. Übermittlung personenbezogener Daten eines Kindes

Die DS-GVO beinhaltet im Unterschied zur DSRL erstmals Regelungen, die die besondere Behandlung der Verarbeitung von personenbezogenen Daten eines Kindes bis zum dreizehnten Lebensjahr normieren.[166] Eine nähere Beleuchtung dieser Regelungen erscheint für die Zwecke dieser Arbeit jedoch nicht notwendig.

2.3.5. Übermittlung sensibler Daten

Die erste Unterscheidung des Artikel 9 DS-GVO zum bisherigen Artikel 8 DSRL ist die ausdrückliche Erwähnung von genetischen, biometrischen und Daten über Strafurteile.

Gleich bleibt hingegen das generelle Verarbeitungsverbot für sensible Daten, dem unmittelbar eine Aufzählung von Ausnahmetatbeständen folgt. Diese decken sich weitestgehend mit den Ausnahmetatbeständen des Artikel 8 DSRL, insofern bringt die DS-GVO in diesem Regelungsbereich keine Änderung mit sich. Neuerungen werden sich jedoch allenfalls aufgrund der nun direkten Anwendbarkeit der Verordnung und der damit verbundenen Entbehrlichkeit von Umsetzungsgesetzen ergeben. Für die österreichische Rechtslage ist in diesem Zusammenhang beachtlich, dass bisher einige der Ausnahmetatbestände aus der DSRL nicht ordnungsgemäß im DSG umgesetzt wurden. So ist die Anführung der Ausnahme für indirekt personenbezogene Daten [167] nicht von der DSRL gedeckt. Indirekt personenbezogene Daten erfüllen jedoch – nachdem bei solchen die dahinter stehende Person zumindest bestimmbar ist – schon bisher die Definition der personenbezogenen Daten der DSRL.[168] Insofern war auch Artikel 8 der DSRL auf indirekt personenbezogene Daten anzuwenden, wobei dieser jedoch eine Privilegierung – wie in § 9 Abs 2 DSG vorgesehen – nicht kennt. Aufgrund dieses Normenkonfliktes kommt es zum Anwendungsvorrang der DSRL, deren Bestimmungen daher unmittelbare Anwendbarkeit entfalten.[169] Die Verarbeitung sensibler indirekt personenbezogene Daten ist daher – wenn keine anderen Ausnahmetatbestände verwirklicht sind – nicht zulässig.

Auch bei den Ausnahmetatbeständen des § 9 Z 7 und Z 8 DSG weist die Umsetzung Unterschiede zur europarechtlichen Vorgabe in Art 8 DSRL auf.

Im gegenständlichen Zusammenhang ist dies deswegen von Relevanz, weil mangels Umsetzungsgesetz das Ziel, nämlich die direkte Anwendbarkeit der europarechtlichen

[166] Art 8 DS-GVO.
[167] § 9 Z 2 DSG.
[168] Art 2 lit a DSRL.
[169] *Jahnel*, Handbuch Datenschutzrecht, Rz 4/72.

Vorgaben, nicht erst über richtlinienkonforme Interpretation oder den Anwendungsvorrang der Richtlinie gegenüber nationalem (Verfassungs-)Recht erreicht wird.

2.3.6. Benachrichtigungspflicht bei Berichtigungen und Löschungen

Auch beim Datentransfer innerhalb der EU legt die DS-GVO den für die Verarbeitung Verantwortlichen – wenn sie Daten weitergegeben haben – die Pflicht auf, die Empfänger von allfällig vorgenommenen Berichtigungen[170] oder Löschungen[171] von Daten zu informieren.[172] Diese Pflicht besteht unabhängig davon, ob die Empfänger der Daten im Inland, EU-Ausland oder in Drittstaaten sitzen. Damit soll neben der Transparenz der Datenvorgänge vor allem eine Abgleichung der beider Orts gespeicherten Daten erreicht werden.

2.4. Datentransfer in Drittstaaten

Der Transfer personenbezogener Daten sowohl in andere Mitgliedstaaten als auch in Drittstaaten nimmt rasant zu. Die EU hat sich zum Ziel gesetzt, alle Betroffenen bei der Übermittlung personenbezogener Daten in Drittländer in gleichem Maße zu schützen und sieht sich selbst als die geeignete Ebene hierzu.[173]

Vor diesem Hintergrund wurde zur Regelung des Datentransfers in Drittländer und an Internationale Organisationen ein eigenes Kapitel V in die DS-GVO aufgenommen. In dessen Rahmen behandeln die Artikel 40 bis 45a sowohl Drittländer und deren Teilbereiche (regionale Gebiete oder einzelne Verarbeitungssektoren), in denen die Empfänger ansässig sind, als auch Internationale Organisationen als Empfänger gleich. Die nachfolgenden Ausführungen stellen – zur besseren Lesbarkeit – lediglich allgemein auf *„Empfänger in Drittstaaten“* ab, gelten jedoch gleichermaßen für Empfänger in deren Teilbereichen und Internationale Organisationen. Lediglich dort, wo eine unterschiedliche Behandlung von Empfängern in Drittländern und Internationalen Organisationen vorgesehen ist, wird differenziert.

2.4.1 Grundsätze

In einem ersten Entwurf der Europäischen Kommission – noch vor der ersten veröffentlichten, gegenständlich als *„Kommissionsentwurf“* bezeichneten Fassung KOM

[170] Art 16 DS-GVO.
[171] Art 17 DS-GVO.
[172] Art 13 DS-GVO.
[173] KOM (2012) 11 endg., 6.

(2012) 11 endg. – war zunächst beabsichtigt, die zulässige Weitergabe von Daten an Drittstaaten nur auf der Grundlage europäischen Rechts oder darauf beruhender Rechtshilfeabkommen zu erlauben. Dies ließ sich jedoch infolge intensiver Lobbyarbeit und Einflussnahme der amerikanischen Regierung vorerst nicht aufrecht halten und ist folglich auch nicht Teil des öffentlich vorgestellten Kommissionsentwurfes geworden.[174]

Kapitel V der DS-GVO legt zunächst die allgemeinen Grundsätze fest, wann und unter welchen Voraussetzungen eine Datenübermittlung in Drittländer zulässig sein soll. Wenig überraschend wird die Zulässigkeit einer Übermittlung von personenbezogenen Daten in Drittländer an die Einhaltung der Bestimmungen des Kapitels V geknüpft.[175] Das bedeutet, dass mindestens einer der im Folgenden[176] dargestellten Rechtfertigungsgründe vorliegen muss.

Artikel 40 DS-GVO wird von einem interessanten Satz eingeleitet. In diesem wird – etwas missverständlich – festgehalten, dass nur eine Übermittlung jener persönlichen Daten von Schutzbereich umfasst sind, die bereits verarbeitet werden oder deren Verarbeitung nach der Übermittlung im Drittland geplant ist. Weder die Erwägungsgründe noch die englische Originalfassung – letztere, weil sie wörtlich übersetzt wurde – liefern Aufschlussgründe, weshalb nicht etwa bloß auf eine Übermittlung personenbezogener Daten abgestellt wird.

Nun sind zunächst generell kaum Sachverhalte vorstellbar, in denen eine Übermittlung von Daten erfolgen soll, die noch nicht verarbeitet sind. Verarbeitung im Sinne der DS-GVO sind beinahe sämtliche im Vorfeld einer Übermittlung denkbare Vorgänge, wie bereits das Erheben, Erfassen, das Ordnen, Speichern oder die Bereitstellung von Daten, wobei auf eine automationsunterstützte Verarbeitungsweise ausdrücklich nicht abgestellt wird.[177] Aus den gleichen Gründen ist ebenfalls keine Übermittlung denkbar, in deren (meist sogar unmittelbarem) Nachgang die Daten nicht verarbeitet werden würden. Jede Datenübermittlung erfolgt mit dem Ziel des Zugangs der Daten beim Empfänger. Ist aber bereits das Erheben, Erfassen, das Ordnen, Speichern, Auslesen oder Abfragen eine Verarbeitung iSd Artikels 3 DS-GVO, ist fraglich, welchen Vorgang ein Empfänger setzen könnte, der nicht unter den Verarbeitungsbegriff fällt.

---

[174] *Albrecht*, Datenschutzgrundverordnung in 10 Punkten vom 22.10.2013, 2; <www.janalbrecht.eu/fileadmin/material/Dokumente/221013_DS-Pressebriefing_Dt..pdf > (24.08.2014).
[175] Art 40 DS-GVO.
[176] Siehe sogleich 2.4.2.
[177] Art 3 DS-GVO.

Zudem – und vor allem – ist die Datenübermittlung selbst als Verarbeitung definiert, weshalb Daten, die übermittelt werden schon begrifflich automatisch auch verarbeitet werden. Insofern ist keine Übermittlung von Daten in Drittländer ersichtlich, die von Artikel 40 – und damit den Bestimmungen des Kapitel V – nicht erfasst wäre.

Unerheblich ist auch, ob die Daten von einem für die Verarbeitung Verantwortlichen oder von einem Auftragsverarbeiter übermittelt werden, zumal beide Rollen zwar erwähnt, jedoch nicht unterschiedlich behandelt werden. Auch auf Empfängerseite unterscheidet die DS-GVO nicht, ob die Daten einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter übermittelt werden. Zur daher nicht mehr relevanten Unterscheidung zwischen Übermittlung und Überlassen (iSd DSG) siehe oben.[178]

In konsequenter Weise sind von diesen Grundsätzen auch die Weitergabe personenbezogener Daten von Verarbeitern in Drittländern an Verarbeiter in weiteren Drittländern umfasst.

2.4.2. Die einzelnen Zulässigkeitsgrundlagen

a. Übermittlung nach Angemessenheitsbeschluss

Der erste Tatbestand der DS-GVO, bei dessen Verwirklichung eine Datenübermittlung in Drittländer zulässig ist, ist keine große Neuerung. Wie schon Artikel 25 Abs 1 DSRL sieht der nunmehrige Artikel 41 DS-GVO in seinem ersten Absatz die Möglichkeit vor, dass Daten jederzeit übermittelt werden dürfen, wenn das betreffende Empfängerdrittland bzw auch bloß ein regionaler oder organisatorischer Teilbereich ein angemessenes Schutzniveau aufweist. In diesem Fall bedarf es auch keiner weiteren Genehmigung.[179]

Die entsprechenden Kriterien, die bei der Prüfung der Angemessenheit des Schutzniveaus zu beachten (und vom Empfängerstaat zu erfüllen) sind, liefert die DS-GVO gleich selbst mit.[180] Abgestellt werden soll vor allem auf den Rechtsrahmen im Drittland inklusive der Durchsetzbarkeit der aus diesem erwachsenden Ansprüche für die betroffenen Personen[181] und die Existenz unabhängiger Aufsichtsbehörden.[182] Im Vergleich zum Kommissionsentwurf holt der Vorschlag des LIBE-Ausschusses auch ausdrücklich die Rechtsprechung mit ins Boot und ergänzt die Auflistung um die juristischen Präzedenzfälle.

---

[178] Siehe oben 2.3.2.
[179] Art 41 Abs 1 DS-GVO.
[180] Vgl Art 41 Abs 2 DS-GVO.
[181] Art 41 Abs 2 lit a DS-GVO.
[182] Art 41 Abs 2 lit b DS-GVO.

Ausdrücklich betont wird die Möglichkeit der Europäischen Kommission, sowohl die Existenz als auch das Nichtvorhandensein eines angemessenen Datenschutzniveaus in einem Drittland mittels delegierten Rechtsakts nach Maßgabe von Artikel 86 DS-GVO festzustellen. [183] Im Kommissionsvorschlag war noch der Erlass von Durchführungsrechtsakten gemäß Artikel 87 Abs 2 vorgesehen. Vor Erlass eines solchen Rechtsaktes hat die Kommission jedoch den – nach der DS-GVO neu einzurichtenden – Europäischen Datenschutzausschuss [184] um Stellungnahme zum Datenschutzniveau im entsprechenden Drittland zu ersuchen.[185]

Unabhängig vom Ausgang der Überprüfung ist das Ergebnis der Adäquanzentscheidung in einer Liste im Amtsblatt der Europäischen Union und – seit dem Vorschlag des LIBE-Ausschusses – auch auf deren Website zu veröffentlichen. Dadurch wird den für die Verarbeitung Verantwortlichen oder Auftraggebern jederzeit ein aktueller Überblick über die Möglichkeit einer Rechtfertigung der Datenübermittlung aufgrund eines gegebenen Angemessenheitsbeschlusses gewährt.[186] Für den Fall, dass von einem delegierten Rechtsakt mit Bescheinigung eines angemessenen Schutzniveaus der Verarbeitungssektor eines Drittlandes betroffen ist, hat der Rechtsakt ein Verfallsdatum zu enthalten.

Auch die Möglichkeit eines negativen Angemessenheitsbeschlusses stellt keine Neuerung im Vergleich zur DSRL dar, die dies in ihrem Artikel 4 vorsieht. Lediglich die unmittelbare Folge, der negative Eintrag in die Liste im Amtsblatt bzw auf der Webseite der Europäischen Union, ist neu. Bisher wurde bei einem Negativbeschluss den Mitgliedstaaten lediglich die Pflicht auferlegt, Datenübermittlungen in das betroffene Drittland zu verhindern. Weiterhin möglich ist jedoch selbst bei einem negativen Beschluss die Rechtfertigung des Datentransfers über eine der anderen Zulässigkeitsgrundlagen.

Nach Inkrafttreten der DS-GVO sorgt eine Übergangsregelung dafür, dass die Europäische Kommission für bereits überprüfte Drittländer keine erneute Adäquanzentscheidung treffen muss. Die bisherigen Angemessenheitsbeschlüsse, die die Kommission auf Basis des Artikel 25 Abs 4 (kein angemessenes Schutzniveau) oder Abs 6 (angemessenes Schutzniveau) DSRL getroffen hat, bleiben solange aufrecht, bis die Kommission sie aufhebt oder einen

[183] Art 41 Abs 3 bzw Abs 5 DS-GVO.
[184] Art 64 ff DS-GVO.
[185] Art 41 Abs 6a DS-GVO.
[186] Art 41 Abs 7 DS-GVO.

entgegenlautenden Beschluss fällt. Längstens jedoch fünf Jahre nach Inkrafttreten der Verordnung, dann erlischt die Wirksamkeit dieser Beschlüsse jedenfalls.[187]

In Summe halten durch Artikel 41 DS-GVO die Regelungen des bisherigen Artikel 25 DSRL Einzug in die Datenschutzgrundverordnung. Abgesehen von den Adaptierungen, die durch die unmittelbare Geltung der Verordnung zu treffen waren, werden hier keine nennenswerten Veränderungen vorgenommen.

b. Übermittlung bei angemessenen Garantien

Wie schon die DSRL[188] sieht auch die DS-GVO die Möglichkeit vor, Datenübermittlungen in Drittländer, bei denen die Kommission kein angemessenes Datenschutzniveau festgestellt oder bei denen noch keine derartige Überprüfung stattgefunden hat, durch die Vereinbarung geeigneter Garantien zum Schutz der personenbezogenen Daten zu rechtfertigen.[189]

Die Verordnung nennt auch – nicht abschließend – vier Sachverhalte, bei deren Verwirklichung das Bestehen geeigneter Garantien angenommen wird:

Erstens versichert die Existenz verbindlicher unternehmensinterner Vorschriften, sofern sie den Anforderungen des Artikel 43 DS-GVO entsprechen, solche geeigneten Garantien.[190]

Zweitens sollen für die Verarbeitung Verantwortliche oder Auftraggeber stets Daten in Drittländer übermitteln dürfen, wenn und solange sie über ein gültiges europäisches Datenschutzsiegel[191] verfügen.

Drittens führt die Verwendung von Standarddatenschutzklauseln im Rahmen der Vertragsbeziehung zwischen Übermittler und Empfänger zur Zulässigkeit des Datentransfers. Wie auch bei den Angemessenheitsbeschlüssen wird im Vorschlag des LIBE-Ausschusses der Kommission die ursprünglich vorgesehene Möglichkeit von Durchführungsrechtsakten – diesfalls zur Annahme von Standarddatenschutzklauseln – verwehrt. Die ursprüngliche Bestimmung (Artikel 42 Abs 2 lit b DS-GVO) sollte der Kommission ermöglichen, Standarddatenschutzklauseln nach Durchführung eines Ausschussverfahrens anzunehmen. Im Entwurf des LIBE-Ausschusses ist dieser Unterpunkt (lit b) nicht mehr enthalten, sodass eine Annahme der Klauseln durch die Kommission ohne Einbindung einer Aufsichtsbehörde nicht

[187] Art 41 Abs 8 DS-GVO.
[188] Art 26 Abs 2 DSRL.
[189] Art 42 Abs 1 DS-GVO.
[190] Siehe unten 2.4.2.c
[191] Art 39 1e DS-GVO.

mehr möglich ist. Zwar enthält der LIBE-Entwurf in Artikel 42 Abs 3 nach wie vor einen Verweis auf Artikel 42 Abs 2 lit b, was jedoch als Übertragungsfehler zu qualifizieren ist. In der englischsprachigen Version jedenfalls wurde der Verweis auf die entfallene lit b in konsequenter Weise ebenfalls gestrichen.[192]

Standarddatenschutzklauseln können daher – ohne besondere Genehmigung – nur dann zur Erbringung geeigneter Garantieren herangezogen werden, wenn sie zuvor von einer Aufsichtsbehörde infolge eines durchgeführten Kohärenzverfahrens nach Maßgabe des Artikel 57 angenommen wurden. Durchführungsrechtsakte der Kommission werden insofern dennoch benötigt, als die Kommission solchen Standarddatenschutzklauseln (unabhängig der Annahme durch die Aufsichtsbehörde) allgemeine Gültigkeit zuerkennen muss.[193] Die Festlegung der Standarddatenschutzklauseln durch eine Aufsichtsbehörde mit anschließender Gültigerklärung durch die Kommission ist eine der Neuerungen in der DS-GVO.

Änderungen an den Klauseln dürfen – zur zulässigen Berufung auf diesen Rechtfertigungstatbestand – keine vorgenommen worden sein. Dies entspricht der bereits bisherigen Rechtslage, die diese Vorgabe aus den in der DSRL enthaltenen Erwägungsgründen zu den Standardvertragsklauseln kennt.[194] Diese Erwägungsgrunde werden nun in den Regelungsteil der Verordnung aufgenommen. Umgekehrt sollen die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter keinesfalls daran gehindert werden, den Standarddatenschutzklauseln zusätzliche Klauseln hinzuzufügen bzw sie in umfangreichere Verträgen zu implementieren. Der Formulierung des entsprechenden Erwägungsgrundes ist zu entnehmen, dass es sich bei letzterem beinahe um eine Art Wunschvorstellung handelt – solange freilich dadurch keine Widersprüche zu den vorgegebenen Klauseln generiert werden.[195]

Als vierten und letzten Sachverhalt, der eine geeignete Garantie darstellen kann, erwähnt Art 42 Abs 2 DS-GVO die Vereinbarung von (eigenen) Vertragsklauseln zwischen Übermittler und Empfänger. Werden jedoch solche individuell vereinbarte Klauseln – anstatt der angenommenen Standarddatenschutzklauseln – verwendet, bedürfen sie einer vorherigen Genehmigung durch eine Aufsichtsbehörde.[196] Für den Fall, dass die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche auch Personen in zumindest einem

[192] General Data Protection Regulation, European Parliament first reading, amendment 138, article 42.
[193] Vgl Art 62 Abs 1 lit b DS-GVO.
[194] Siehe oben 1.4.3.c.
[195] ErwGr 84 DS-GVO.
[196] Art 42 Abs 1 lit d DS-GVO.

anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Datenverkehr haben, ist wiederum das Kohärenzverfahren entsprechend des Artikel 57 DS-GVO durchzuführen.[197]

Artikel 42 Abs 5 sah im Kommissionsentwurf für den Fall, dass keine geeignete Garantien in einem rechtsverbindlichen Instrument vorgesehen wurden, die Möglichkeit vor, bei der zuständigen Aufsichtsbehörde eine Genehmigung gemäß Artikel 34 Abs 1 DS-GVO einzuholen, um die Daten dennoch übermitteln zu können. Diese Möglichkeit wurde im Vorschlag des LIBE-Ausschusses (ebenso wie Art 34 Abs 1) gestrichen. Hinzugefügt wurde vielmehr eine Übergangsregelung durch die ausdrückliche Anweisung, dass Genehmigungen, die von Aufsichtsbehörden vor dem Inkrafttreten der DS-GVO auf Basis des korrelierenden Artikel 26 Abs 2 DSRL getroffen wurden, solange gültig bleiben, bis diese Aufsichtsbehörde sie ändert, ersetzt oder aufhebt; längstens jedoch zwei Jahre ab Inkrafttreten der Verordnung.[198]

c. Übermittlung aufgrund unternehmensinterner Vorschriften

Gänzlich neu – jedenfalls im Vergleich zur DSRL – ist die Aufnahme von verbindlichen unternehmensinternen Vorschriften als explizite Grundlage für die Zulässigkeit einer Datenübermittlung. Die Tür zur Rechtfertigung des Datentransfers durch verbindliche unternehmensinterne Vorschriften stößt Artikel 42 DS-GVO durch den entsprechenden Verweis in Abs 2 lit a auf.

Die Europäische Union reagiert damit – ähnlich wie der österreichische Gesetzgeber durch die DSG-Novelle 2010 [199] – auf die entsprechenden Entwicklungen und Unternehmensstrukturen am Wirtschaftssektor. Die stets zunehmenden und wachsenden internationalen Großkonzerne tätigen zur Abwicklung der (internen) Geschäftsabläufe zahlreiche grenzüberschreitende Datenübermittlungen eines verbundenen Unternehmens oder einer Niederlassung an entsprechende Pendants in Drittländer. Als Reaktion auf gegebenen Praktiken sowie die Anforderungen der Aufsichtsbehörden war eine eigene Ausgestaltung dieses Rechtfertigungsgrundes unumgänglich.[200] Eine Verpflichtung der Unternehmen zum Abschluss von (Standard-)Vertragsklauseln innerhalb der eigenen Unternehmensgruppe wäre überschießend und würde an den tatsächlichen Gegebenheiten vorbeizielen. Daher hält die für

[197] Art 42 Abs 4.
[198] Art 42 Abs 5 DS-GVO.
[199] Siehe oben 1.4.3.d.
[200] Vgl KOM (2012) 11 endg., 13.

solche Fälle bisher nur national vorgesehene Möglichkeit von Binding Corporate Rules durch Artikel 43 DS-GVO nunmehr Einzug in das Unionsrecht.

Definiert werden die verbindlichen unternehmensinternen Vorschriften in Artikel 4 Z 17 DS-GVO als Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet.

Wie sich bereits aus dem Namen des Rechtfertigungsgrundes ergibt, steht dieser (nur) für unternehmensinterne Vorgänge offen. Die Artikel-29-Datenschutzgruppe lieferte bereits zur Rechtslage nach der DSRL Anleitungen, was unter *„unternehmensintern“* zu verstehen sei. Demnach muss es sich um Vorschriften handeln, die von multinationalen Unternehmen eingeführt wurden, für die in der Regel die Zentrale zuständig ist.[201] Auf diesen Rechtfertigungsgrund können sich nur Mitglieder einer Unternehmensgruppe berufen, wenn sie tatsächlich zur Einhaltung dieser Vorschriften verpflichtet sind. Diese Verbindlichkeit muss sowohl unternehmensintern – etwa über entsprechende Verhaltenskodizes oder Bedrohung mit Disziplinarsanktionen – als auch in Bezug auf die Außenwelt, dh auch auf die rechtliche Durchsetzbarkeit der Vorschriften durch die betroffenen Personen, gegeben sein.[202]

Selbstredend, dass diese verbindlichen unternehmensinternen Vorschriften einen gewissen Mindestinhalt und – vor allem – Mindestschutz aufweisen müssen. Zur Anwendung sollen daher nur jene Vorschriften gelangen, deren geeignete Garantie eines entsprechenden Datenschutzniveaus durch eine vorab erteilte Genehmigung der Aufsichtsbehörde bestätigt worden ist.[203]

Sowohl der Kommissionsvorschlag als auch der Vorschlag des LIBE-Ausschusses qualifizieren die Annahme von verbindlichen unternehmensinternen Vorschriften als Angelegenheit mit allgemeiner Geltung.[204] Aus diesem Grund hat das Prüfverfahren zur Genehmigung von vorgelegten unternehmensinternen Vorschriften nach Maßgabe des Kohärenzverfahrens in Artikel 58 DS-GVO zu erfolgen. Insbesondere bedeutet dies, dass im Unterschied zum Kohärenzverfahren nach Artikel 57 DS-GVO der Europäische

---

[201] *Artikel-29-Datenschutzgruppe:* Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer vom 03.06.2003, 11639/02/DE, WP 74, 8 <www.cnpd.public.lu/de/publications/groupe-art29/wp074_de.pdf> (24.08.2014).
[202] *Artikel-29-Datenschutzgruppe*, WP 74, Punkt 3.3.
[203] ErwGr 85 DS-GVO.
[204] Art 58 Abs 2 lit f DS-GVO.

Datenschutzausschuss[205] miteinzubeziehen ist. Beabsichtigt eine nationale Aufsichtsbehörde die Annahme von verbindlichen unternehmensinternen Vorschriften, hat sie diese Absicht zuvor der Kommission und dem Europäischen Datenschutzausschuss bekannt zu geben.[206] Daran hat sich unverzüglich ein vollständiger Austausch sämtlicher zweckdienlicher Informationen (Sachverhalt, geplante Maßnahme, Begründung, etc.) zwischen den Aufsichtsbehörden, der Kommission und dem Datenschutzausschuss einzustellen,[207] bevor dieser eine Stellungnahme abgibt.[208]

Ist das Kohärenzverfahren durchgeführt, kann die nationale Aufsichtsbehörde die verbindlichen unternehmensinternen Vorschriften unter bestimmten Voraussetzungen genehmigen:

Zunächst haben diese Vorschriften Rechtsverbindlichkeit für alle Mitglieder der Unternehmensgruppe des für die Verarbeitung Verantwortlichen, deren Subunternehmer und Beschäftigte, zu entfalten und müssen von diesen auch angewendet werden.[209] Die Übertragung von durchsetzbaren Rechten an die betroffenen Personen ist zudem ausdrücklich in den Vorschriften festzuhalten.[210] Für die Verarbeitung von Daten über Beschäftigte sind – allerdings erst seit dem Vorschlag des LIBE-Ausschusses – bei der Erarbeitung von unternehmensinternen Vorschriften die Arbeitnehmervertreter beizuziehen.[211]

Hinsichtlich des Inhaltes legt die DS-GVO ebenfalls Mindestanforderungen fest. So haben die unternehmensinternen Vorschriften jedenfalls Angaben über die Struktur- und Kontaktdaten der Unternehmensgruppe, die Art der zu übermittelnden personenbezogenen Daten und der betroffenen Person, Art und Zweck der Datenverarbeitung, das/die betreffende/n Drittland/Drittländer sowie die allgemeinen Datenschutzgrundsätze (Zweckbindung, Datenminimierung, begrenzte Aufbewahrungsfristen, Rechtsgrundlage für die Verarbeitung sowie Bestimmungen für etwaige Verarbeitung sensibler Daten, etc.) zu enthalten. Ebenso – und insbesondere – müssen die Rechtsverbindlichkeit der unternehmensinternen Vorschriften und Informationen über die Rechte der betroffenen Personen inklusive deren Durchsetzbarkeit festgehalten sein.[212]

---

[205] Art 64 ff DS-GVO.
[206] Art 58 Abs 1 DS-GVO.
[207] Art 58 Abs 5 und 6 DS-GVO.
[208] Art 58 Abs 6a DS-GVO.
[209] Art 43 Abs 1 lit a DS-GVO.
[210] Art 43 Abs 1 lit b DS-GVO.
[211] Art 43 Abs 1a DS-GVO.
[212] Art 43 Abs 2 lit a bis e DS-GVO.

Werden von für die Verarbeitung Verantwortlichen, die in einem Mitgliedstaat der EU niedergelassen sind, Haftungen für Verstöße gegen die unternehmensinternen Vorschriften durch nicht in Mitgliedsstaaten niedergelassene Mitglieder der Unternehmensgruppe übernommen, sind diese ebenfalls anzugeben.[213]

Schließlich haben die unternehmensinternen Vorschriften für ihre eigene Einhaltung zu sorgen. Aus diesem Grund ist in den Vorschriftstext aufzunehmen, wie die Verfahren zur Überprüfung der Einhaltung der Vorschriften durchgeführt und die diesbezügliche Zusammenarbeit mit der Kommission abzulaufen hat.[214]

Die Kommission wiederum ist berechtigt, die Kriterien und die Anforderungen, die verbindliche unternehmensinterne Vorschriften zur Erreichung einer Genehmigung erfüllen müssen, festzulegen.[215] In einem zwischenzeitlichen Berichtsentwurf war dafür noch der Datenschutzausschuss vorgesehen.

d. Europäisches Datenschutzsiegel

Als völlige Neuerung ist in der DS-GVO zusätzlich zu den bereits bisher bekannten Rechtfertigungsgründen eine freiwillige Zertifizierung von Unternehmen vorgesehen, die den transnationalen Datentransfer im Sinne einer vorab erteilten Genehmigung erleichtern würde.[216] Es handelt sich dabei um ein standardisiertes Datenschutzzeichen, das die DS-GVO als Europäisches Datenschutzsiegel bezeichnet und das jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter bei jeder Aufsichtsbehörde in der Europäischen Union gegen Entgelt (*„angemessene Gebühr“*) beantragen kann.[217] Damit soll neben der Erleichterung der Datenübermittlung auch eine erhöhte Transparenz und verbesserte Einhaltung der DS-GVO verbunden sein.[218]

Die Aufsichtsbehörden haben im Rahmen der ihnen obliegenden Überprüfung, ob die Antragsteller den Anforderungen entsprechen, mit dem Europäischen Datenschutzausschuss zusammenzuarbeiten und gegebenenfalls auch auf externe Prüfer zurückzugreifen.[219]

---

[213] Art 43 Abs 2 lit f DS-GVO.
[214] Art 43 Abs 2 lit i bis k DS-GVO.
[215] Art 43 Abs 3 DS-GVO.
[216] *Waidmann*, ecolex 2014, 7.
[217] Art 39 Abs 1a DS-GVO.
[218] ErwGr 77 DS-GVO.
[219] Art 39 Abs 1c und 1d DS-GVO.

e. Übermittlung oder Weitergabe, die nicht im Einklang mit dem Unionsrecht stehen

Beinahe jeder Gesetzgebungsprozess der Europäischen Union wird von intensivem Lobbyismus begleitet – teilweise durch Mitgliedsstaaten, teilweise durch Drittstaaten. Im Fall der DS-GVO sieht sich der europäische Gesetzgebungsprozess aufgrund der weitreichenden, globalen Auswirkungen starker versuchter Einflussnahme auch aus Drittstaaten ausgesetzt. Aufgrund des konträren Zugangs zum Datenschutz und der damit potenziell verbundenen Auswirkungen auf US-Unternehmen in Europa intervenieren vor allem die USA relativ stark.

Besonders plakativ lässt sich das anhand der nunmehr als Artikel 43a im Vorschlag des LIBE-Ausschusses enthaltenen Bestimmungen veranschaulichen. Diesen liegt als Ausgangslage der Sachverhalt zu Grunde, dass Gerichte oder Verwaltungsbehörden aus Drittstaaten durch Urteile oder sonstige Entscheidungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern die Übermittlung personenbezogener Daten verlangen. Bereits im einem ersten Entwurf der Kommission – noch vor KOM (2012) 11 endg. – war für diesen Fall ausschließlich die Anwendbarkeit europäischen Datenschutzrechtes vorgesehen. Infolge der Einflussnahme der USA findet sich diese Bestimmung jedoch nicht im ersten öffentlich vorgestellten Kommissionsentwurf. Zu begründen ist dies offensichtlich mit den Bedenken der Vereinigten Staaten, mit diesem Artikel wäre eine Rechtsunsicherheit für US-Unternehmen bei Überwachungsmaßnahmen verbunden.

Das Europäische Parlament jedenfalls hat diesen Artikel (vormals Art 42) im Vorschlag des LIBE-Ausschusses (nun als Art 43a) wieder hinzugefügt.

Nach derzeitigem Stand würde daher auch in dem Fall, dass US-Gerichte oder US-Verwaltungsbehörden von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern personenbezogene Daten verlangen, im Anwendungsbereich[220] der DS-GVO europäisches Datenschutzrecht zur Anwendung gelangen. Dies gilt für sämtliche Drittstaaten, sofern kein Abkommen über Amtshilfe vorhanden ist oder zwischen diesen und dem betreffenden Mitgliedsstaat, in dem der Adressat des Urteils oder der Entscheidung sitzt, kein entsprechendes geltendes internationales Übereinkommen abgeschlossen wurde.[221]

Derartige Urteile oder Entscheidungen werden keinesfalls anerkannt oder vollstreckt. Eine Übermittlung von personenbezogenen Daten in Entsprechung solcher Urteile oder Entscheidungen kann nur nach vorheriger Genehmigung durch die Aufsichtsbehörde, die der

[220] Siehe oben 2.1.
[221] Vgl Art 43a Abs 1 DS-GVO.

für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter einzuholen hat, erfolgen.[222] Die Aufsichtsbehörde hat bei ihrer Prüfung, ob eine derartige Genehmigung erteilt wird, insbesondere zu untersuchen, ob die Weitergabe gemäß Artikel 44 Abs 1 lit d und e sowie Artikel 44 Abs 5 DS-GVO erforderlich und rechtlich vorgeschrieben ist.[223]

Das Schicksal auch dieses Artikels wird Inhalt der Trialog-Verhandlungen sein. Aufgrund der in diesem Punkt konträren Positionen zwischen Kommission und Parlament ist in diesem Punkt jedoch erhöhte Spannung gegeben.

f. Weitere Rechtfertigungsgründe

Schlussendlich sieht die DS-GVO – wie schon die DSRL[224] und in weiterer Folge das österreichische DSG[225] – eine Auffangregelung vor, welche Sachverhalte aufzählt, bei deren Verwirklichung eine Datenübermittlung in Drittstaaten selbst bei Fehlen eines Angemessenheitsbeschlusses und von geeigneten Garantien zulässig ist.

Entsprechend der Konzeption der Vorgängerbestimmung in der DSRL handelt es sich auch bei Artikel 44 DS-GVO um eine taxative Aufzählung. Selbst der Inhalt und die Reihenfolge ist beinahe ident mit jenem des Artikel 26 Abs 1 DSRL. Lediglich Artikel 26 Abs 1 lit d DSRL wurde in zwei einzelne Aufzählungspunkte aufgeteilt, weshalb die DS-GVO nun einen Unterpunkt (lit a – g) mehr aufweist als die DSRL.

Als einzige nennenswerte inhaltliche Neuerung war im Kommissionsentwurf eine weitere Ausnahmebestimmung enthalten, der zu Folge auch bereits ein überwiegendes berechtigtes Interesse des Übermittelnden die Zulässigkeit einer Datenübermittlung begründen hätte können.[226] Allerdings sollte diese Möglichkeit nur für Datenübermittlungen zur Verfügung stehen, die weder als häufig noch als massiv gelten.[227] Demnach wäre eine Datenübermittlung zulässig gewesen, wenn sie zur Verwirklichung eines berechtigten Interesses des (übermittelnden) für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters erforderlich gewesen wäre. Zusätzlich hätte der für die Verarbeitung Verantwortliche bzw der Auftragsverarbeiter jedoch alle Umstände beurteilen und gegebenenfalls geeignete Garantien zum Schutz der persönlichen Daten einholen müssen.

---

[222] Art 43a Abs 2 DS-GVO.
[223] Art 43a Abs 3 DS-GVO; siehe sogleich 2.4.2.f.
[224] Artikel 26 Abs 1 DSRL.
[225] § 12 Abs 3 DSG.
[226] Art 44 Abs 1 lit h idF KOM (2012) 11 endg.
[227] ErwGr 88 DS-GVO.

Nähere Ausführungen, welche Umstände einer Überprüfung unterzogen hätten werden müssen, waren jedoch weder im Verordnungstext noch in den Erwägungsgründen enthalten. Jedenfalls darf als problematisch angesehen werden, dass diese Bestimmung – insbesondere die letzteren beiden Tatbestandsmerkmale – die Beurteilung der Notwendigkeit einer Einholung geeigneter Garantien dem für die Verarbeitung Verantwortlichen bzw dem Auftragsverarbeiter übertragen hätte, was ein erhöhtes Ausmaß von Rechtsunsicherheit erwarten hätte lassen. Dieser Ausnahmetatbestand ist jedoch im nun vorliegenden Entwurf des LIBE-Ausschusses nicht mehr enthalten. Wenn er daher im Zuge der Trailog-Verhandlungen nicht wieder aufgenommen wird, erübrigt sich die obige Diskussion ohnehin.

Es bleibt daher bei den grundsätzlich bereits aus der DSRL bekannten Rechtfertigungsgründen:

- Die Zustimmung der betroffenen Person.[228]
- Die Notwendigkeit zur Vertragserfüllung des Betroffenen mit dem für die Verarbeitung Verantwortlichen (gilt nicht für nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen).[229]
- Die Notwendigkeit zu einem im Interesse der betroffenen Person liegenden Vertragsabschluss bzw einer entsprechenden Vertragserfüllung zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten (gilt nicht für nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen).[230]
- Die Notwendigkeit der Datenübermittlung aufgrund eines öffentlichen Interesses. Dieses Interesse muss dabei im Unionsrecht oder im Recht des Mitgliedsstaates, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.[231]
- Die Übermittlung ist zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich.[232]
- Die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich.[233] Dieser Rechtfertigungsgrund ist schon in Artikel 26 Abs 1 lit e DSRL enthalten, wurde nun aber mit dem Zusatz versehen, dass die betroffene Person aus physischen oder rechtlichen Gründen außerstande sein muss, ihre Einwilligung abzugeben. Diese zusätzliche Voraussetzung, die die DSRL schon

[228] Art 44 Abs 1 lit a DS-GVO.
[229] Art 44 Abs 1 lit b iVm Abs 4 DS-GVO.
[230] Art 44 Abs 1 lit c iVm Abs 4 DS-GVO.
[231] Art 44 Abs 1 lit d iVm Abs 5 DS-GVO.
[232] Art 44 Abs 1 lit e DS-GVO.
[233] Art 44 Abs 1 lit f DS-GVO.

im Rechtfertigungsgrund für die Verarbeitung von sensiblen Daten in Artikel 8 Abs 2 lit c kennt, ist im Vergleich zur DSRL neu. Physische Gründe könnten etwa in der Ohnmächtigkeit liegen, rechtliche in einer mangelnden Geschäftsfähigkeit.[234]

- Beinahe wortgleich aus der DSRL wurde auch der Rechtfertigungsgrund der Übermittlung aus einem öffentlichen Register übernommen. Öffentlich bedeutet in diesem Zusammenhang, dass in das Register entweder die gesamte Öffentlichkeit oder zumindest Personen, die ein berechtigtes Interesse nachweisen können, einsehen können müssen.[235] Im zweiten Fall, also jenem der eingeschränkten Öffentlichkeit, darf die Übermittlung zudem nur dann erfolgen, wenn sie von einer dieser Personen, die ein berechtigtes Interesse haben, beantragt wurde oder diese Empfänger der Übermittlung ist. Als weitere Einschränkung dürfen die Datenübermittlungen nicht die Gesamtheit der Daten oder ganze Kategorien der im Register enthaltenen Daten umfassen.[236]

Zusammenfassend spiegelt Artikel 44 DS-GVO die Ausnahmetatbestände, die bereits in Artikel 26 Abs 1 DSRL enthalten waren – abgesehen von der zusätzlichen Voraussetzung der unmöglichen Zustimmung bei den lebenswichtigen Interessen der betroffenen oder einer anderen Person – wider. Die einzige potenzielle Neuerung, eine mögliche Abwägung der Schutzinteressen der betroffenen Person mit den berechtigten Interessen des für die Verarbeitung Verantwortlichen oder des Auftraggebers im Rahmen von geringfügigen und vereinzelt stattfindenden Datenübermittlungen, wurde vom Europäischen Parlament im Vergleich zum Kommissionsentwurf jedoch vorerst wieder verworfen.

2.4.4. Genehmigungspflicht im Rahmen der Rechtfertigungsgrundlagen

Übermittlungen von personenbezogenen Daten in Drittländer, denen die Kommission ein angemessenes Datenschutzniveau konstatiert hat, bedürfen keiner weiteren Genehmigung durch eine Aufsichtsbehörde. Ebenso Datenübermittlungen, die nach Maßgabe eines europäischen Datenschutzsiegels erfolgen.

Werden Standarddatenschutzklauseln oder verbindliche unternehmensinterne Vorschriften der Übermittlung zu Grunde gelegt, bedarf es grundsätzlich ebenfalls keiner zusätzlichen besonderen Genehmigung.[237] Selbstverständlich müssen beide Rechtfertigungsinstrumente

[234] Vgl *Jahnel*, Handbuch Datenschutzrecht, Rz 4/80.
[235] Art 44 Abs 1 lit g DS-GVO.
[236] Art 44 Abs 2 DS-GVO.
[237] Art 42 Abs 3 DS-GVO.

entsprechend der jeweiligen Bestimmungen zustande gekommen sein. Das bedeutet, dass die Aufsichtsbehörde sowohl bei den Standarddatenschutzklauseln (über die Annahme infolge des Kohärenzverfahrens)[238] als auch bei den verbindlichen unternehmensinternen Vorschriften (über deren Genehmigungspflicht)[239] einzubinden ist.

Einzig eine Übermittlung auf Basis individueller, zwischen den für die Verarbeitung Verantwortlichen bzw. Auftragsverarbeitern einerseits und den Empfängern andererseits vereinbarter Vertragsklauseln[240] bedarf einer zusätzlichen Genehmigung. Sollen diese als Rechtfertigungsgrundlage herangezogen werden, müssen diese Klauseln durch die zuständige Aufsichtsbehörde genehmigt werden.[241] Diese Genehmigung hat der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter einzuholen.

2.4.5. Weitere Regelungen im Zusammenhang mit dem Datentransfer ins Ausland

a. Informationspflichten

Beabsichtigt der für die Verarbeitung Verantwortliche, die Daten an ein Drittland zu übermitteln, muss er die betroffene Person zuvor davon unterrichten. Ebenso muss in diesen Fällen mitgeteilt werden, ob ein Angemessenheitsbeschluss der Kommission vorliegt oder nicht. Soll der Datentransfer durch geeignete Garantien – insbesondere durch Verwendung von Standarddatenschutzklauseln oder verbindliche unternehmensinterne Vorschriften – gerechtfertigt werden, ist die betroffene Person zusätzlich von diesen Garantien sowie von der Möglichkeit, eine Kopie davon zu erhalten, in Kenntnis zu setzen.[242]

Der Entwurf des LIBE-Ausschusses sieht letztere Informationspflichten über die Garantien auch für den Fall von Übermittlungen nach Artikel 44 Abs 1 lit h DS-GVO vor. Dieser Verweis, der sowohl in der deutschsprachigen als auch der englischsprachigen Version enthalten ist, muss jedoch als Redaktionsfehler angesehen werden, zumal der Unterpunkt lit h in beiden Versionen gestrichen wurde.

Im Zuge des Gesetzgebungsprozesses kam es zu einer geringfügigen Änderung der Formulierung: Der Entwurf des LIBE-Ausschusses spricht von einer *„Unterrichtung“* der betroffenen Person, wohingegen der Kommissionsvorschlag die Pflicht zur *„Information“*

---

[238] Art 42 Abs 1 lit c DS-GVO.
[239] Art 43 Abs 1 DS-GVO.
[240] Art 42 Abs 1 lit d DS-GVO.
[241] Siehe oben 2.4.2.b.
[242] Art 14 Abs 1 lit g DS-GVO.

beinhaltete. Sollte aus dieser Umformulierung tatsächlich eine Änderung in der Qualität der Mitteilung ersehen werden können (die englischsprachigen Versionen beider Vorschläge sprechen jeweils von *„information to the data subject“*), muss sie als Erhöhung der Anforderungen an die Form der Mitteilung gesehen werden. Tatsächlich jedoch ist mMn die geänderte Wortwahl der Betonung der Unterscheidung vom im LIBE-Entwurf neu eingefügten Artikel 13a, der mit *„Standardisierte Informationsmaßnahmen“* übertitelt ist, geschuldet. Die Unterrichtung jedenfalls hat spätestens zum Zeitpunkt der ersten Weitergabe zu erfolgen.[243]

Gleichzeitig werden zahlreiche Ausnahmen von der Pflicht zur Unterrichtung normiert, die sich im Großen und Ganzen mit jenen der DSRL[244] decken. Insbesondere, wenn die Datenverarbeitung zu historischen, statistischen oder wissenschaftlichen Forschungszwecken durchgeführt werden soll, entfällt die Unterrichtungspflicht, wenn sie unmöglich oder mit unverhältnismäßig hohem Aufwand verbunden wäre. Als Neuerung im LIBE-Entwurf wurde dies jedoch an die weitere Voraussetzung, dass die Daten für jedermann zugänglich veröffentlicht wurden, gebunden.[245]

Ebenso besteht in Fällen, in denen die Weitergabe der Daten ausdrücklich in einem Gesetz geregelt ist, keine Pflicht zur Unterrichtung. Im Unterschied zur DSRL stellt die DS-GVO jedoch bestimmte Anforderungen an ein solches Gesetz. Selbstredend ist, dass der für die Verarbeitung Verantwortliche diesem unterliegen muss. Entscheidend ist, dass das Gesetz auch Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person vorsehen muss. Die Qualität und der Umfang solcher Maßnahmen muss dabei auf die jeweilige Datenverarbeitung und die Art der personenbezogenen Daten abgestimmt sein.[246]

b. Dokumentationspflicht

Das Grundbestreben der DS-GVO, eine erhöhte Transparenz bei den Datenverarbeitungen zu schaffen, spiegelt sich auch in Artikel 28 wider. Dort wird den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern die Pflicht auferlegt, ihre Datenverarbeitungen umfassend zu dokumentieren.[247] Während der Kommissionsentwurf die Informationen über die Datenübermittlungen ausdrücklich als Mindestinformation anführte,

[243] Art 14 Abs 4 lit b DS-GVO.
[244] Art 11 Abs 2 DSRL.
[245] Art 14 Abs 5 lit b DS-GVO.
[246] Art 14 Abs 5 lit c DS-GVO.
[247] Art 28 Abs 1 DS-GVO.

die dokumentiert werden musste,[248] ist dies im Entwurf des LIBE-Ausschusses nicht mehr explizit aufgelistet. In der Regel wird eine Dokumentation der Datenübertragungen jedoch notwendig sein, um die Pflichten, die den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern auferlegt werden, zu erfüllen.

c. Verhaltensregeln

Ebenso wie bereits die DSRL[249] hält auch die DS-GVO die Absicht fest, die Mitgliedsstaaten und die Kommission – nun gemeinsam mit den Aufsichtsbehörden – zur Zusammenarbeit anzuhalten, um Verhaltensregeln auszuarbeiten, die zur ordnungsgemäßen Anwendung der DS-GVO beitragen sollen. Auf die jeweiligen Erfordernisse in den einzelnen Datenverarbeitungen soll dabei Rücksicht genommen werden. Datenübermittlungen in Drittstaaten sind dabei als einer der Bereiche, die jedenfalls im Rahmen dieser Verhaltensregeln behandelt werden sollen, explizit aufgelistet.[250]

d. Verbot durch die Aufsichtsbehörde – Sanktionen

Steht dies im Einklang mit der DS-GVO, können die Aufsichtsbehörden die Datenübermittlung in Drittstaaten unterbinden.[251] Neben dem bereits in der DSRL[252] enthaltenen Recht zur Klagsführung, steht den Aufsichtsbehörden nunmehr auch die Möglichkeit offen, Ordnungswidrigkeiten nach Artikel 79 DS-GVO zu ahnden.[253] Die nationalen Aufsichtsbehörden verfügen damit über eine eigene Sanktionsmöglichkeit,[254] die – wie explizit betont wird – gleichzeitig verhältnismäßig und abschreckend wirken muss.[255] Die DS-GVO gibt den Aufsichtsbehörden zwar die Wahlmöglichkeit zwischen verschiedenen Sanktionen, legt aber gleichzeitig fest, dass bei Verstößen jedenfalls eine davon auszuüben ist.[256] Das Spektrum reicht dabei von schriftlichen Verwarnungen über regelmäßige Überprüfungen bis hin zu – teils beträchtlichen – Geldbußen.

Vor allem hinsichtlich der Höhe dieser Geldbußen darf das Ergebnis der Trialog-Verhandlungen mit Spannung erwartet werden, zumal diesbezüglich die bisherigen Entwürfe aufgrund einiger zwischenzeitlicher Änderungen zueinander enorme Abweichungen

[248] Art 18 Abs 2 lit f idF KOM (2012) 11 endg.
[249] Art 27 DSRL.
[250] Art 28 Abs 1 lit f DS-GVO.
[251] Art 53 Abs 1 lit h DS-GVO.
[252] Art 28 Abs 3, dritter Spiegelstrich DSRL.
[253] Art 53 Abs 4 DS-GVO.
[254] *Engel*, Die EU-Datenschutz-Grundverordnung: Was sich ändert, was bleibt – Teil II, jusIT 5/2013, 179.
[255] Art 79 Abs 2 DS-GVO.
[256] Art 79 Abs 2a DS-GVO.

aufweisen. Der Kommissionsentwurf kannte hinsichtlich der Deckelung der Geldbußen noch Abstufungen: Je nachdem, gegen welche Bestimmung der DS-GVO verstoßen werde, konnten Geldbußen von € 250.000,00, € 500.000,00 und € 1,000.000,00 – bzw. im Fall von Unternehmen bis zu 0,5%, 1% und 2% des weltweiten Jahresumsatzes – verhängt werden.[257] Diese Abstufung ist im Entwurf des LIBE-Ausschusses nicht mehr enthalten. Vielmehr wurden die betraglichen Obergrenzen erheblich anbehoben und liegen nunmehr bei € 100,000.000,00 bzw. – im Fall von Unternehmen – bei 5% des weltweiten Jahresumsatzes; je nachdem, welcher Betrag höher ist.[258]

Unabhängig davon, welche Höchstgrenzen nun die tatsächliche Endfassung der DS-GVO aufweist, ist bereits abzusehen, dass das Sanktionssystem im Vergleich zur bisherigen Rechtslage[259] für die Pflichtverletzenden mit deutlich spürbareren Strafen ausgestattet ist. Es ist davon auszugehen, dass dies in den Unternehmen, die Daten ins Ausland oder in Drittstaaten übertragen, zweifellos zu erhöhter Sensibilisierung und zur Ergreifung entsprechender Maßnahmen zur Einhaltung eines angemessenen Datenschutzniveaus führen wird.

[257] Art 79 Abs 4, 5 und 6 idF KOM (2012) 11 endg.
[258] Art 79 Abs 2a lit c DS-GVO.
[259] Siehe oben 1.4.3.f.

3. Ergebnis / Schlussfolgerungen

Die Datenschutzreform der Europäischen Union und insbesondere die DS-GVO werden seit mehreren Jahren und vielerorts als großer Wurf mit einschneidenden Neuerungen angekündigt. Die Frage, ob dies auch für den Datentransfer ins Ausland gilt, war Inhalt der obigen Ausführungen und wird nach folgender zusammenfassender Übersicht beantwortet:

3.1. Die Neuerungen der DS-GVO

3.1.1. Unmittelbare Anwendbarkeit

Die weitreichendste Neuerung der Datenschutzgrundverordnung liegt in der unmittelbaren Anwendbarkeit in den Mitgliedsstaaten und ist daher eine strukturelle. Mit der automatisch damit verbundenen Entbehrlichkeit nationaler Umsetzungsgesetze sind nicht nur eine Harmonisierung der europäischen Datenschutzregelungen, sondern in vielen Bereichen Erleichterungen verbunden.

Nach Inkrafttreten der DS-GVO erübrigt sich jedenfalls innerhalb des EWR die Frage nach dem anzuwendenden Recht.[260] Zudem werden die Probleme, die bisher aufgrund der Unschärfen im Rahmen der Umsetzung der DSRL mit dem DSG aufgetreten sind, beseitigt.[261]

Für die österreichische Rechtsordnung bedeutet dies insbesondere, dass einerseits mit der Ausweitung des Schutzbereiches auf Daten juristischer Personen und andererseits mit der Unterscheidung zwischen Übermittlung und Überlassung von Daten zwei typische Eigenheiten, die infolge (zulässiger) Abweichung von der DSRL im DSG enthalten sind, wegfallen. Dies ist zwar keine inhaltliche Neuerung auf europäischer Regelungsebene (schon die DSRL kannte beide Punkte nicht), sondern entfaltet durch die nunmehrige direkte Anwendbarkeit und – vor allem – das Umsetzungsverbot betreffend den durch die Verordnung geregelten Bereich Auswirkunken auf das national geltende Recht.[262]

3.1.2. Räumlicher und sachlicher Anwendungsbereich

Wie soeben erwähnt, sind die Daten juristischer Personen nicht vom Schutzbereich der DS-GVO umfasst und kann infolge des Umsetzungsverbotes auf nationaler Ebene ihr Schutz nicht aus den europarechtlichen Vorgaben abgeleitet werden.

---

[260] Siehe oben 2.1.
[261] Siehe oben 2.3.3. und 2.3.5.
[262] Siehe oben 2.2.

Neben dem sachlichen Schutzbereich entfaltet die DS-GVO auch Auswirkungen auf den räumlichen Anwendungsbereich. Diesbezüglich stellt die DS-GVO differenziertere Regelungen als bisher die DSRL auf. Zunächst werden alle Datenverarbeitungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern mit einer Niederlassung in der EU – sofern die Verarbeitung dieser Niederlassung dient – dem Schutz der DS-GVO unterstellt. Der Ort dieser Verarbeitung, insbesondere dass diese innerhalb der EU erfolgt, ist dabei irrelevant. Umgekehrt erfolgt insbesondere eine Eingrenzung des Schutzbereiches, zumal Datenverarbeitungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern aus Drittstaaten nur dann unter den Schutzbereich des DS-GVO fallen, wenn Daten von in der EU ansässigen Personen verarbeitet werden und die Verarbeitung explizit auf diese Personen ausgerichtet ist.[263]

3.1.3. Datentransfer innerhalb der EU

Im Großen und Ganzen orientiert sich die DS-GVO bei den Zulässigkeitsvoraussetzungen von Datenverarbeitungen sensibler und nicht-sensibler Daten an den bisherigen Vorgaben in der DSRL. Nachdem Datenübermittlungen jeweils unter die Legaldefinition einer Datenverarbeitung fallen, sind auch diesbezüglich auf europarechtlicher Ebene kaum Neuerungen zu erkennen. Aufgrund der teilweisen Abweichung des österreichischen DSG von der DSRL bedeutet eine wortgleiche Übernahme der europarechtlichen Vorgaben in die DS-GVO gleichzeitig eine Neuerung in der nationalen Rechtsordnung. Insbesondere im Rahmen mancher Rechtfertigungsgründe lässt sich dies verdeutlichen.[264]

Inhaltlich sind zwischen der DSRL und der DS-GVO kaum Änderungen zu ersehen. Lediglich die besonderen Datenarten, wie die personenbezogenen Daten von Kindern und – im Rahmen der sensiblen Daten nunmehr ausdrücklich erwähnten – biometrischen und genetischen Daten sowie Daten über Strafurteile stellen eine Neuerung dar.

Im Bereich der nicht-sensiblen Daten stellt die DS-GVO nunmehr klar, dass eine Rechtsgrundlage, soll sie zur Rechtfertigung einer Datenverarbeitung herangezogen werden, entweder im Unionsrecht oder im Recht des betreffenden Mitgliedsstaates liegen muss.[265]

---

[263] Siehe oben 2.1.
[264] Siehe oben 2.3.3. und 2.3.5.
[265] Siehe oben 2.3.3.

3.1.4. Datentransfer in Drittstaaten

Ebenso wie schon die DSRL kennt auch die DS-GVO mehrere Rechtfertigungsgründe, die zu einer Zulässigkeit eines Datentransfers in Drittstaaten führen können.

Der erste dieser Rechtfertigungsgründe, die Übermittlung infolge Angemessenheitsbeschlusses, ist beinahe ident mit der Regelung in der DSRL. Selbst der negative Angemessenheitsbeschluss war bereits Inhalt der DSRL, lediglich dessen automatische Folge, der negative Eintrag in den Publikationsmedien der EU kann als Neuerung angesehen werden.[266]

Ebenso ist die Möglichkeit, die Zulässigkeit des Datentransfers über die Vereinbarung von Standarddatenschutzklauseln keine inhaltliche Neuerung, wenngleich nunmehr ausdrücklich im Regelungsteil der DS-GVO angeführt.[267]

Die DSRL hingegen kannte keine Möglichkeit, über die Verabschiedung verbindlicher unternehmensinterner Vorschriften die Empfänger in der eigenen Unternehmensgruppe zur Einhaltung eines angemessenen Datenschutzniveaus zu verpflichten. Dennoch wäre es vermessen, diesen nun ausdrücklich in der DS-GVO enthaltenen Rechtfertigungsgrund als Neuerung zu qualifizieren, zumal er bereits Einzug in die nationalen Rechtsordnungen gehalten hat.[268] Neu sind hingegen die Ausgestaltung der Anforderungen, denen solche unternehmensinterne Vorschriften genügen müssen, und die Festlegung des Genehmigungsverfahrens – vor allem die zwingende Einbeziehung des (ebenfalls neuen) Datenschutzausschusses.[269]

Gänzliches Neuland beschreitet die DS-GVO durch die Installierung eines europäischen Datenschutzsiegels, dessen Inhaber dadurch über eine Art Vorabgenehmigung für den Datentransfer ins Ausland verfügen.[270]

Der nunmehr vom Europäischen Parlament wieder eingefügte Artikel 43a DS-GVO stellt inhaltlich keine Änderung gegenüber der bisherigen Rechtslage dar, wie auch der EuGH im eingangs erwähnten Vorabentscheidungsverfahren festzustellen haben wird.[271]

---

[266] Siehe oben 2.4.2.a.
[267] Siehe oben 2.4.2.b.
[268] Siehe oben 1.4.3.d.
[269] Siehe oben 2.4.2.c.
[270] Siehe oben 2.4.2.d.
[271] Siehe oben Seite 4.

3.1.5. Weitere Regelungen im Zusammenhang mit dem Datentransfer ins Ausland

Neben wenigen inhaltlichen Änderungen bei den Rechtfertigungsgründen, kennen auch die weiteren Regelungen, die den transnationalen Datentransfer berühren, lediglich kleinere Adaptierungen im Vergleich zur DSRL – etwa im Rahmen der Informationspflichten.[272] Markant sind die Neuerungen jedoch im Sanktionssystem, das in Zukunft für Pflichtverletzer deutlich schmerzhaftere Höchststrafen kennt, die nun auch – durch Koppelung an den Jahresumsatz – auf die wirtschaftliche Stärke der Unternehmen Bezug nehmen.

3.2. Fazit

Die obige Zusammenfassung und die dieser zu Grunde liegende nähere Betrachtung des Kapitels über den Datentransfer ins Ausland lässt keinen andere Erkenntnis zu als festzustellen, dass die DS-GVO in diesem Bereich kaum umfassende inhaltliche Neuerungen im Vergleich zur DSRL aufweist.

Die nennenswerten Neuerungen für den transnationalen Datentransfer ergeben sich nicht aus den Bestimmungen, die den Datentransfer selbst regeln. Vielmehr entfalten die Ausgestaltung der europarechtlichen Vorgaben als direkt anwendbare Verordnung sowie neue allgemeine Instrumente – wie etwa der Europäische Datenschutzausschuss und das Europäische Datenschutzsiegel – Auswirkungen auch auf den Bereich des Datentransfers ins Ausland.

Wird daher die Datenschutz-Grundverordnung als innovatives Kernstück einer umfassenden Datenschutzreform bezeichnet, muss dies jedenfalls für den Regelungsbereich des Datentransfers ins Ausland relativiert werden. Weder wartet die DS-GVO mit einschneidenden inhaltlichen Neuerungen auf noch ist eine nennenswerte Stärkung der Betroffenenrechte zu erwarten.

[272] Etwa die Anforderungen, die an ein Gesetz gestellt werden, wenn bei der Weitergabe von Daten aufgrund dieses Gesetzes eine Unterrichtung der betroffenen Person unterbleiben soll. Siehe oben 2.4.5.a.

Literaturverzeichnis

- *Bauer Lukas, Reimer Sebastian* (Hrsg), Handbuch Datenschutzrecht (facultas 2009)
- *Dohr Walter/Pollierer Hans J/Weiss Ernst M/Knyrim Rainer* (Hrsg), DSG. Datenschutzrecht² (Manz 16. ErgLfg 2014)
- *Engel Christoph*, Die EU-Datenschutz-Grundverordnung: Was sich ändert, was bleibt, Teil 1, JusIT 2013/65
- *Engel Christoph*, Die EU-Datenschutz-Grundverordnung: Was sich ändert, was bleibt, Teil 2, JusIT 2013/86
- *Gola Peter*, Datenschutz-Jahrbuch[23] 2014 (Datakontext 2014)
- *Jahnel Dietmar* (Hrsg), Datenschutz und E-Government, Jahrbuch 2012 (NWV Neuer Wissenschaftlicher Verlag 2012)
- *Jahnel Dietmar*, Handbuch Datenschutzrecht (Jan Sramek Verlag 2010)
- *Lachmayer Konrad*, Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, ÖJZ 2012/92
- *Pollierer Hans J/Weiss Ernst M/Knyrim Rainer* (Hrsg), DSG. Datenschutzrecht² (Manz 2014)
- *Schaar Peter:* Europäischer Startschuss für die Datenschutzreform: Eine Chance für wirksame Verbesserungen, Datenschutz und Datensicherheit – DuD 03/2012.
- *Waidmann Teresa*, Konzerninterner Austausch personenbezogener Daten, ecolex 2014, 7
- <ec.europa.eu/justice/data-protection/index_de.htm>
- <http://www.cnpd.public.lu/de/publications/groupe-art29>
- <www.janalbrecht.eu>

Anhang I

Kurzzusammenfassung / Abstract

Kurzzusammenfassung

Die Europäische Union unterzieht die europäischen Datenschutzvorschriften derzeit einer umfassenden Novellierung. Startschuss dieser Datenschutzreform war der von der Europäischen Kommission am 25.01.2012 vorgestellte Entwurf für eine Datenschutz-Grundverordnung, die als Kernstück der Reform nicht nur inhaltliche Neuerungen, sondern auch einen Systemwechsel bringen wird.

Zunächst wird die Europäische Union im Bereich des allgemeinen Datenschutzrechts vom Zusammenspiel einer europäischen Richtlinie mit den nationalen Umsetzungsgesetzen abgehen und eine in den Mitgliedsstaaten direkt anwendbare Verordnung erlassen. Damit sollen nicht nur Auslegungs- und Umsetzungsschwierigkeiten beseitigt, sondern anstatt der einzelnen nationalen – naturgemäß unterschiedlichen – Datenschutzgesetze ein einheitliches Datenschutzniveau geschaffen werden. Am 21.11.2013 reichte der Ausschuss des Europäischen Parlamentes für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) seinen Entwurf für die Europäische Datenschutz-Grundverordnung ein, der im Vergleich zur Ausgangsversion der Europäischen Kommission in zahlreichen Punkten bedeutende Änderungen aufwies. Dieser Entwurf wurde am 12.03.2014 von den EU-Abgeordneten akzeptiert und dient einerseits als Grundlage für die Trialog-Verhandlungen zwischen Europäischem Parlament, Europäischer Kommission und dem Rat der Europäischen Union sowie andererseits als Basis der gegenständlichen Arbeit.

Eine Verabschiedung der Datenschutz-Grundverordnung vor dem Jahr 2015 ist zwar aus heutiger Sicht unrealistisch, dennoch soll die gegenständliche Arbeit zum ehest möglichen Zeitpunkt jene Vorschriften der Datenschutz-Grundverordnung untersuchen, die in Zukunft den Datentransfer ins Ausland regeln. Die entsprechenden Artikel werden auf inhaltliche Neuerungen und deren Auswirkungen im Vergleich zur aktuellen Rechtslage durchleuchtet.

Am Ende dieser näheren Untersuchung gelangt die Arbeit zum ernüchternden Ergebnis, dass die Datenschutz-Grundverordnung jedenfalls im Rahmen dieses Themenbereichs kaum umfassende inhaltliche Neuerungen im Vergleich zur bisherigen EU-Datenschutzrichtlinie aufweist. Die nennenswerten Neuerungen für den transnationalen Datentransfer ergeben sich nur bedingt aus den inhaltlichen Bestimmungen betreffend den Datentransfer selbst. Vielmehr ergeben sich die nachhaltigsten Auswirkungen aufgrund neuer allgemeiner Instrumente (etwa dem Europäischen Datenschutzausschuss) sowie – und vor allem – aus der nunmehr gewählten Ausgestaltung der europarechtlichen Vorgaben als direkt anwendbare Verordnung.

Abstract

Proposed by the European Union, the European data protection is being subject to major amendments at the moment. Starting point of the data protection reform was a draft of a General Data Protection Regulation which was presented by the European Commission on 25. 01. 2012. A central element are not only revisions with regard to content. As a consequence it will also bring about a shift in the (current) stystem.

At first the European Union is going to diverge from the interplay of an EU Directive and ist implementation in national law systems. A regulation, directly applicable in European member states, is going to be issued. On the one hand it aims at eliminating difficuties in the interpretation and implementation arising from different data protection acts specific to the member states. On the other hand it intends to create a EU-wide standardized level of data protection. On 21. 11. 2013 the European Parliament Committee on Civil Liberties, Justice and Home Affairs submitted its draft of the General Data Protection Regulation. Compared to the initial draft of the European Commission, this draft showed significant changes in numerous matters. It was accepted by the EU delegates on 12. 03. 2014 and serves as a basis for negotiations in trialogues between the European Parliament, the European Commission and the Council of the European Union. It is also the basis for this master's degree thesis.

From today's perspective a passing of the General Data Protection Regulation before 2015 seems unrealistic. Nevertheless the current draft is worth taking a closer look at due to the emerging cornerstones. This academic paper examines those regulations of the General Data Protection Regulation which are going to regulate transfer of data abroad at the earliest possible time. The relevant articles are examined for reforms in terms of content and their effects in comparison to the current legal position.

As a result of these close examinations, this thesis arrives at some rather sobering conclusions. With regards to the subject area of this paper, the General Data Protection Regulation does not contain extensive amendments in terms of content compared to the current EU Data Protection Directive. Reforms worth mentioning concerning transnational data transfer only result to a certain extent from the regulations of data transfer itself. It is rather new, general instruments (such as the European Data Protection Board) that bring about lasting effects. Particularly they result from the now chosen structure of an EU Regulation as a directly applicable regulation.

Anhang II

Bearbeitete Regelungen der Datenschutz-Grundverordnung

(auszugsweise)

Artikel 3

Räumlicher Anwendungsbereich

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

2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung

a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist; oder

b) der Überwachung dieser betroffenen Personen dient.

3. Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck

(1) *entfällt im Vergleich zum Vorschlag der Kommission vom 25.01.2012 (COM(2012)0011)*

(2) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer eindeutigen Kennung oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen, sozialen oder geschlechtlichen Identität dieser Person sind;

(7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden;

(7a) „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

(17) „verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet;

Artikel 6

Rechtmäßigkeit der Verarbeitung

1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.

b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.

c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.

d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.

e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.

f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen – oder, im Fall der Weitergabe, der berechtigten Interessen eines Dritten, an den die Daten weitergegeben wurden – , die die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllen, erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.

3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e müssen eine Rechtsgrundlage haben im

a) Unionsrecht oder

b) Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.

Die einzelstaatliche Regelung muss ein im öffentlichen Interesse liegendes Ziel verfolgen der zum Schutz der Rechte und Freiheiten Dritter erforderlich sein, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem mit der Verarbeitung verfolgten legitimen Zweck stehen. Im Rahmen dieser Verordnung können im Recht der Mitgliedstaaten Einzelheiten der Rechtmäßigkeit der Verarbeitung, insbesondere zu den für die Verarbeitung Verantwortlichen, zur Zweckbestimmung der Verarbeitung und Zweckbindung, zur Art der Daten und zu den betroffenen Personen, zu Verarbeitungsvorgängen und -verfahren, zu Empfängern sowie zur Speicherdauer geregelt werden.

Artikel 9 Abs 1

Besondere Datenkategorien

1. Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, sexuelle Orientierung oder Geschlechtsidentität oder die Mitgliedschaft und Betätigung in einer Gewerkschaft

hervorgehen, sowie von genetischen oder biometrischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten oder mutmaßliche Straftaten, Verurteilungen oder damit zusammenhängende Sicherungsmaßregeln ist untersagt.

Artikel 26 Abs 1 und Abs 2

Auftragsverarbeiter

1. Der für die Verarbeitung Verantwortliche wählt für jede in seinem Auftrag durchzuführende Verarbeitung einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.

2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können ihre jeweiligen Funktionen und Aufgaben in Bezug auf die Anforderungen dieser Verordnung festlegen und sehen vor, dass der Auftragsverarbeiter:

a) nur auf Weisung des für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeitet, es sei denn, in Rechtsvorschriften der Union oder der Mitgliedstaaten ist etwas anderes bestimmt;

b) ausschließlich Mitarbeiter beschäftigt, die sich zur Vertraulichkeit verpflichtet haben oder der gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle in Artikel 30 genannten erforderlichen Maßnahmen ergreift;

d) sofern nichts anderes bestimmt ist, die Bedingungen festlegt, unter denen die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf,

e) soweit es verarbeitungsbedingt möglich ist, in Absprache mit dem für die Verarbeitung Verantwortlichen die geeigneten und zweckmäßigen technischen und organisatorischen Voraussetzungen dafür schafft, dass der für die Verarbeitung Verantwortliche seine Pflicht erfüllen kann, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) den Auftragsverarbeiter bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen unterstützt;

g) nach Abschluss der Verarbeitung dem für die Verarbeitung Verantwortlichen sämtliche Ergebnisse zurückgibt, die personenbezogenen Daten auf keine andere Weise weiterverarbeitet und bestehende Kopien löscht, es sei denn, in Rechtsvorschriften der Union oder der Mitgliedstaaten ist die Speicherung der Daten vorgesehen;

h) dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen für den Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Nachprüfungen vor Ort zulässt.

Artikel 13

Benachrichtigungspflicht bei Berichtigungen und Löschungen

Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung, die aufgrund von Artikel 16 beziehungsweise 17 vorgenommen wird, mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 14

(auszugsweise)

Unterrichtung der betroffenen Person

1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche, nach der Bereitstellung der Hinweise gemäß Artikel 13a, zumindest Folgendes mit,

g) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission, oder im Falle der in Artikel 42, Artikel 43 und Artikel 44 Absatz 1 Buchstabe h erwähnten Übermittlungen einen Verweis auf die entsprechenden Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten,

[...]

4. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1, 2 und 3

b) falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, zum Zeitpunkt ihrer Erfassung oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen, unter denen die Daten erhoben oder auf sonstige Weise verarbeitet wurden, Rechnung trägt, oder, falls die Weitergabe an einen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe, oder, wenn die Daten für die Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Kommunikation mit dieser Person;

[...]

5. Die Absätze 1 bis 4 finden in folgenden Fällen keine Anwendung:

a) Die betroffene Person verfügt bereits über die Informationen gemäß den Absätzen 1, 2 und 3 oder

b) die Daten werden vorbehaltlich der in Artikel 81 oder Artikel 83 genannten Bedingungen und Garantien für historische, statistische oder wissenschaftliche Forschungszwecke verarbeitet, und werden nicht bei der betroffenen Person erhoben und die Unterrichtung erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohen Aufwand verbunden und der für die Verarbeitung

Verantwortliche hat die Informationen so veröffentlicht, dass sie von jedermann abgefragt werden können, oder

c) die Daten werden nicht bei der betroffenen Person erhoben und die Erfassung oder Weitergabe ist ausdrücklich in einem Gesetz geregelt, dem der für die Verarbeitung Verantwortliche unterliegt und das unter Berücksichtigung der aufgrund der Verarbeitung und der Art der personenbezogenen Daten bestehenden Risiken angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht,

Artikel 28 Abs 1

Dokumentation

1. Alle für die Verarbeitung Verantwortlichen und alle Auftragsverarbeiter halten die zur Erfüllung der in dieser Verordnung festgelegten Anforderungen notwendige Dokumentation vor und aktualisieren sie regelmäßig.

Artikel 38 Abs 1 lit f

Verhaltensregeln

1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln oder die Annahme von durch eine Aufsichtsbehörde ausgearbeiteten Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen:

f) Datenübermittlung in Drittländer oder an internationale Organisationen;

Artikel 39 Abs 1a – 1b

Europäisches Datenschutzsiegel

1a. Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung

personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird, insbesondere mit den Grundsätzen der Artikel 5, 23 und 30, den Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter und den Rechten der betroffenen Person.

1b. Die Zertifizierung ist freiwillig, erschwinglich und über ein transparentes und nicht übermäßig aufwändiges Verfahren zugänglich.

1c. Die Aufsichtsbehörden und der Europäische Datenschutzausschuss arbeiten im Rahmen des Kohärenzverfahrens gemäß Artikel 57 zusammen, um ein harmonisiertes datenschutzspezifisches Zertifizierungsverfahren zu gewährleisten, einschließlich harmonisierter Gebühren innerhalb der Union.

1d. Während des Zertifizierungsverfahrens kann die Aufsichtsbehörde spezialisierte dritte Prüfer akkreditieren, die Prüfung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für sie durchzuführen. Dritte Prüfer verfügen über ausreichend Personal, sind unparteiisch und in Bezug auf ihre Aufgaben frei von Interessenskonflikten. Aufsichtsbehörden entziehen die Akkreditierung, wenn es Grund zu der Annahme gibt, dass der Prüfer seine Aufgaben nicht korrekt erfüllt. Die endgültige Zertifizierung erteilt die Aufsichtsbehörde.

1e. Die Aufsichtsbehörden erteilen den für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, denen nach der Prüfung zertifiziert wird, dass sie personenbezogene Daten im Einklang mit dieser Verordnung verarbeiten, das standardisierte Datenschutzzeichen mit der Bezeichnung „Europäisches Datenschutzsiegel“.

1f. Das „Europäische Datenschutzsiegel“ ist so lange gültig, wie die Verarbeitungsprozesse des zertifizierten für die Verarbeitung Verantwortlichen oder des zertifizierten Auftragsverarbeiters weiter vollständig dieser Verordnung entsprechen.

1g. Unbeschadet des Absatzes 1f ist die Zertifizierung höchstens fünf Jahre gültig.

1h. Der Europäische Datenschutzausschuss richtet ein öffentliches elektronisches Register ein, in dem die Öffentlichkeit Einsicht in alle gültigen und ungültigen Zertifikate, die von den Mitgliedstaaten ausgestellt wurden, nehmen kann.

1i. Der Europäische Datenschutzausschuss kann auf eigene Initiative zertifizieren, dass ein technischer Standard zur Verbesserung des Datenschutzes mit dieser Verordnung vereinbar ist.

KAPITEL V
ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

Artikel 40
Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.

Artikel 41
Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

1. Eine Datenübermittlung darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.

2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission

a) die Rechtsstaatlichkeit, die geltenden allgemeinen und sektorspezifischen Vorschriften, insbesondere über die öffentliche Sicherheit, die Landesverteidigung,

die nationale Sicherheit und das Strafrecht, die Umsetzung dieser Rechtsvorschriften, die in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation geltenden Standesregeln und Sicherheitsvorschriften, juristische Präzedenzfälle sowie die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen und insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden;

b) die Existenz und die Wirksamkeit einer oder mehrerer in dem betreffenden Drittland beziehungsweise in der betreffenden internationalen Organisation tätiger unabhängiger Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften, einschließlich hinreichender Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind; und

c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation eingegangenen internationalen Verpflichtungen, insbesondere rechtlich verbindliche Übereinkommen oder Instrumente in Bezug auf den Schutz personenbezogener Daten.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um festzustellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. Diese delegierten Rechtsakte sehen, wenn sie den Verarbeitungssektor betreffen, eine Verfallsklausel vor und werden, sobald ein angemessenes Niveau des Schutzes gemäß dieser Verordnung nicht mehr gewährleistet ist, gemäß Artikel 5 aufgehoben.

4. In jedem delegierten Rechtsakt werden der territoriale und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben.

4a. Die Kommission überwacht laufend die Entwicklungen, die sich auf die in Absatz 2 aufgeführten Faktoren in Drittländern und internationalen Organisationen auswirken könnten, für die delegierte Rechtsakte gemäß Absatz 3 erlassen wurden.

5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um festzustellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bietet oder nicht mehr bietet; dies gilt insbesondere für Fälle, in denen die in dem betreffenden Drittland beziehungsweise der betreffenden internationalen Organisation geltenden allgemeinen und sektorspezifischen Vorschriften keine wirksamen und durchsetzbaren Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für in der Union ansässige betroffene Personen und insbesondere für betroffene Personen, deren personenbezogene Daten übermittelt werden, garantieren.

6. Wenn die Kommission die in Absatz 5 genannte Feststellung trifft, wird dadurch jedwede Übermittlung personenbezogener Daten an das betreffende Drittland beziehungsweise an ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder an die betreffende internationale Organisation unbeschadet der Bestimmungen der Artikel 42 bis 44 untersagt. Die Kommission nimmt zu geeigneter Zeit Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation auf, um Abhilfe für die Situation, die aus dem gemäß Absatz 5 erlassenen Beschluss entstanden ist, zu schaffen.

6a. Vor Erlass der delegierten Rechtsakte gemäß den Absätzen 3 und 5 ersucht die Kommission den Europäischen Datenschutzausschuss um eine Stellungnahme zur Angemessenheit des Datenschutzniveaus. Zu diesem Zweck versorgt die Kommission den Europäischen Datenschutzausschuss mit allen erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlands, Gebiets oder Verarbeitungssektors eines Drittlands oder der internationalen Organisation.

7. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren von Drittländern und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese einen beziehungsweise keinen angemessenen Schutz personenbezogener Daten bieten.

8. Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben fünf Jahre nach Inkrafttreten dieser Verordnung in Kraft, es sei denn, sie wird durch die Kommission vor Ende dieses Zeitraums geändert, ersetzt oder aufgehoben.

Artikel 42

Datenübermittlung auf der Grundlage geeigneter Garantien

1. Hat die Kommission keinen Beschluss nach Artikel 41 erlassen oder hat sie festgestellt, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Datenschutz im Einklang mit Artikel 41 Absatz 5 bietet, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter nur dann personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermitteln, wenn er in einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.

2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere bestehen in Form

a) verbindlicher unternehmensinterner Vorschriften nach Artikel 43; oder

aa) eines gültigen europäischen Datenschutzsiegels gemäß Artikel 39 Absatz 1e für den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter; oder

c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommener Standarddatenschutzklauseln, sofern diesen von der Kommission allgemeine Gültigkeit gemäß Artikel 62 Absatz 1 Buchstabe b zuerkannt wurde, oder

d) von Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden.

3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, aa, b oder c genannten Standarddatenschutzklauseln, eines europäischen Datenschutzsiegels oder unternehmensinternen Vorschriften erfolgen, bedürfen keiner besonderen Genehmigung.

4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung der Aufsichtsbehörde ein. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.

5. Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben zwei Jahre nach Inkrafttreten dieser Verordnung oder so lange in Kraft, es sei denn, sie werden durch die Aufsichtsbehörde vor Ende dieses Zeitraums geändert, ersetzt oder aufgehoben.

Artikel 43

Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften

1. Die Aufsichtsbehörde kann nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens verbindliche unternehmensinterne Vorschriften genehmigen, sofern diese

a) rechtsverbindlich sind, für alle Mitglieder der Unternehmensgruppe des für die Verarbeitung Verantwortlichen oder der externen Subunternehmer, die in den Anwendungsbereich der verbindlichen unternehmensinternen Vorschriften fallen, sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden;

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen;

c) die in Absatz 2 festgelegten Anforderungen erfüllen.

1a. In Bezug auf Beschäftigungsdaten werden die Arbeitnehmervertreter unterrichtet und gemäß Rechtsvorschriften und Praktiken der Union oder der Mitgliedstaaten in die Erarbeitung verbindlicher unternehmensinterner Vorschriften gemäß Artikel 43 einbezogen.

2. Alle verbindlichen unternehmensinternen Vorschriften enthalten mindestens folgende Informationen:

a) Struktur und Kontaktdaten der Unternehmensgruppe und ihrer Mitglieder und der externen Subunternehmer, die in den Anwendungsbereich der verbindlichen unternehmensinternen Vorschriften fallen;

b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Kategorien personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Vorschriften;

d) die allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, die Datenminimierung, begrenzte Aufbewahrungsfristen, die Datenqualität, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, die Rechtsgrundlage für die Verarbeitung sowie die Bestimmungen für etwaige Verarbeitungen sensibler personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese Vorschriften gebundene Organisationen;

e) die Rechte der betroffenen Personen und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen übernommene Haftung für etwaige Verstöße von nicht in der Union niedergelassenen Mitgliedern der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Vorschriften; der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

g) die Art und Weise, wie die betroffenen Personen gemäß Artikel 11 über die verbindlichen unternehmensinternen Vorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;

i) die innerhalb der Unternehmensgruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften;

j) die Verfahren für die Meldung und Erfassung von Änderungen der Unternehmenspolitik und ihre Meldung an die Aufsichtsbehörde;

k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe gewährleisten, wie insbesondere die Offenlegung der Ergebnisse der Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Format, Verfahren, die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung, einschließlich Transparenz für betroffene Personen, und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.

Artikel 43a

Übermittlung oder Weitergabe, die nicht im Einklang mit dem Unionsrecht stehen

1. Unbeschadet eines Abkommens über Amtshilfe oder eines zwischen dem ersuchenden Drittstaat und der Union oder einem Mitgliedstaat geltenden internationalen Übereinkommens werden Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verlangen, personenbezogene Daten weiterzugeben, weder anerkannt noch in irgendeiner Weise vollstreckt.

2. Verlangt ein Urteil eines Gerichts oder eine Entscheidung einer Verwaltungsbehörde eines Drittstaats von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, personenbezogene Daten weiterzugeben, so unterrichtet der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter bzw. ein etwaiger Vertreter des für die Verarbeitung Verantwortlichen die Aufsichtsbehörde unverzüglich über das Ersuchen und muss von der Aufsichtsbehörde die vorherige Genehmigung für die Übermittlung oder Weitergabe erhalten.

3. Die Aufsichtsbehörde prüft die Vereinbarkeit der beantragten Weitergabe mit der Verordnung und insbesondere, ob die Weitergabe gemäß Artikel 44 Absatz 1 Buchstabe d

und e sowie Artikel 44 Absatz 5 erforderlich und rechtlich vorgeschrieben ist. Sind betroffene Personen anderer Mitgliedstaaten betroffen, bringt die Aufsichtsbehörde das in Artikel 57 beschriebene Kohärenzverfahren zur Anwendung.

4. Die Aufsichtsbehörde unterrichtet die zuständige einzelstaatliche Behörde über das Ersuchen. Unbeschadet des Artikels 21 unterrichtet der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter auch die betroffene Person über das Ersuchen und über die Genehmigung der Aufsichtsbehörde sowie gegebenenfalls darüber, ob personenbezogene Daten innerhalb der letzten zwölf aufeinanderfolgenden Monate gemäß Artikel 14 Absatz 1 Buchstabe ha an Behörden übermittelt wurden.

Artikel 44

Ausnahmen

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 vorliegt noch geeignete Garantien nach Artikel 42 bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur zulässig, wenn

a) die betroffene Person der vorgeschlagenen Datenübermittlung zugestimmt hat, nachdem sie über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführter Datenübermittlungen informiert wurde,

b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist,

c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist,

d) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist,

e) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist,

f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

2. Datenübermittlungen gemäß Absatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

4. Absatz 1 Buchstaben b und c gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

5. Das in Absatz 1 Buchstabe d genannte öffentliche Interesse muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.

7. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken in Bezug auf die weitere Festlegung der Kriterien und Bedingungen für die Übermittlung von Daten gemäß Absatz 1 nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b zu veröffentlichen.

Artikel 45

Internationale Zusammenarbeit zum Schutz personenbezogener Daten

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur

a) Entwicklung wirksamer Mechanismen der internationalen Zusammenarbeit, durch die die Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten gewährleistet wird,

b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Mitteilungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,

c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,

d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten,

da) Klärung und Beratung von Zuständigkeitskonflikten mit Drittländern.

2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen und insbesondere zu deren Aufsichtsbehörden, wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese einen angemessenen Schutz bieten.

Artikel 45a

Bericht der Kommission

Die Kommission legt dem Europäischen Parlament und dem Rat spätestens vier Jahre nach dem in Artikel 91 Absatz 1 genannten Termin in regelmäßigen Abständen einen Bericht über die Anwendung der Artikel 40 bis 45 vor. Hierzu kann die Kommission von den Mitgliedstaaten und den Aufsichtsbehörden Informationen einholen, die unverzüglich zu übermitteln sind. Dieser Bericht wird veröffentlicht.

Artikel 53 Abs 1 lit h, Abs 4

Befugnisse

1. Jede Aufsichtsbehörde ist im Einklang mit dieser Verordnung befugt

h) die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation zu unterbinden,

4. Jede Aufsichtsbehörde ist befugt, Ordnungswidrigkeiten nach Artikel 79 zu ahnden. Diese Befugnis wird in einer wirksamen, verhältnismäßigen und abschreckenden Art und Weise ausgeübt.

Artikel 58

Kohärenz in Angelegenheiten mit allgemeiner Geltung

1. Bevor eine Aufsichtsbehörde eine Maßnahme nach Absatz 2 erlässt, übermittelt sie die geplante Maßnahme dem Europäischen Datenschutzausschuss und der Kommission.

2. Die in Absatz 1 genannte Verpflichtung gilt für Maßnahmen, die Rechtswirkung entfalten sollen und

a) entfällt

b) entfällt

c) entfällt

d) der Festlegung von Standard- Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dienen, oder

e) der Genehmigung von Vertragsklauseln gemäß Artikel 42 Absatz 2 Buchstabe d dienen, oder

f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dienen.

3. Jede Aufsichtsbehörde und der Europäische Datenschutzausschuss können beantragen, dass eine Angelegenheit mit allgemeiner Geltung im Rahmen des Kohärenzverfahrens behandelt wird, insbesondere, wenn eine Aufsichtsbehörde die in Absatz 2 genannte geplante Maßnahme nicht vorlegt oder den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht nachkommt.

4. Um die ordnungsgemäße und kohärente Anwendung dieser Verordnung sicherzustellen, kann die Kommission beantragen, dass eine Angelegenheit mit allgemeiner Geltung im Rahmen des Kohärenzverfahrens behandelt wird.

5. Die Aufsichtsbehörden und die Kommission übermitteln unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme und die Gründe, warum eine solche Maßnahme ergriffen werden muss.

6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats die Mitglieder des Datenschutzausschusses und die Kommission über zweckdienliche Informationen, die ihm zugegangen sind. Soweit erforderlich stellt das Sekretariat des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung.

6a. Der Europäische Datenschutzausschuss gibt eine Stellungnahme zu Angelegenheiten, mit denen er gemäß Absatz 2 befasst wird, ab.

7. Der Europäische Datenschutzausschuss kann mit einfacher Mehrheit entscheiden, ob er eine Stellungnahme zu einer gemäß Absatze 3 und 4 vorgelegten Angelegenheit abgibt, wobei zu berücksichtigen ist,

a) ob die Angelegenheit neue Elemente umfasst, wobei rechtliche oder sachliche Entwicklungen berücksichtigt werden, insbesondere in der Informationstechnologie und in Anbetracht des Fortschritts in der Informationsgesellschaft; und

b) ob der Europäische Datenschutzausschuss bereits eine Stellungnahme zu der gleichen Angelegenheit abgegeben hat.

8. Der Europäische Datenschutzausschuss nimmt Stellungnahmen gemäß Artikel 6a und 7 mit der einfachen Mehrheit seiner Mitglieder an. Diese Stellungnahmen werden veröffentlicht.

Artikel 79 Abs 1, 2, 2a

Verwaltungsrechtliche Sanktionen

1. Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen. Die Aufsichtsbehörden arbeiten gemäß Artikel 46 und 57

zusammen, um ein harmonisiertes Niveau der Sanktionen innerhalb der Union zu gewährleisten.

2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.

2a. Die Aufsichtsbehörde verhängt gegen jeden, der seinen in dieser Verordnung festgelegten Pflichten nicht nachkommt, mindestens eine der folgenden Sanktionen:

a) eine schriftliche Verwarnung im Fall eines ersten und nicht vorsätzlichen Verstoßes;

b) regelmäßige Überprüfungen betreffend den Datenschutz;

c) eine Geldbuße, bis zu 100 000 000 EUR oder im Fall eines Unternehmens bis zu 5 % seines weltweiten Jahresumsatzes, je nachdem, welcher der Beträge höher ist.

Artikel 82

Mindestnormen für die Datenverarbeitung im Beschäftigungskontext

1. Die Mitgliedstaaten können im Einklang mit den Regelungen dieser Verordnung und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit durch Rechtsvorschriften die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext, insbesondere, jedoch nicht ausschließlich, für Zwecke der Einstellung und Bewerbung innerhalb des *[richtig: der]* Unternehmensgruppe, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich und tarifvertraglich festgelegten Pflichten gemäß nationalen Rechtsvorschriften oder Gepflogenheiten, des Managements, der Planung und der Organisation der Arbeit, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses regeln. Die Mitgliedstaaten können Kollektivverträge für die weitere Konkretisierung der Vorschriften dieses Artikels vorsehen.

Lebenslauf

Angaben zur Person

Name:	Mag. Martin Führer
Adresse:	1150 Wien, Chrobakgasse 6/10
Nationalität:	Österreich
Geburtsdatum /-ort:	10.07.1984 in Amstetten

Bildungsweg

seit Oktober 2013	Universitätslehrgang für Informations- und Medienrecht am Postgraduate Center der Universität Wien
2004 – 2010	Studium der Rechtswissenschaften an der Rechtswissenschaftlichen Fakultät der Universität Wien
2003 – 2004	Präsenzdienst beim Österreichischen Bundesheer
1998 – 2003	HTBLuVA St. Pölten, Abteilung für EDV und Organisation
1994 – 1998	Bundesrealgymnasium Amstetten
1990 – 1994	VS St. Georgen am Ybbsfelde

Berufserfahrung

2008 – 2011	Redakteur bei den NÖ Nachrichten
2010	Praktikum in der Rechtsabteilung der Sparkasse der Stadt Amstetten
2011	Absolvierung der Gerichtspraxis
seit 2011	Rechtsanwaltsanwärter bei
	urbanek | lind | schmid | reisch rechtsanwälte OG