



universität
wien

DISSERTATION

Titel der Dissertation

„Automatischer Datenaustausch
im Bereich der Finanzdienstleistungen“

verfasst von

Mag. iur. Andreas Fussenegger, LL.M.

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr. iur.)

Wien, 2013

Studienkennzahl lt. Studienblatt:

A 783 101

Dissertationsgebiet lt. Studienblatt:

Rechtswissenschaften

Betreuer:

ao. Univ.-Prof. Mag. Dr. Christian Piska

Vorwort

Meine Dissertation mit dem Titel „Automatischer Datenaustausch im Bereich der Finanzdienstleistungen“ soll dieses viele Themen umfassende Gebiet wissenschaftlich darstellen und dabei besonders rechtliche Lücken und Verbesserungsmöglichkeiten aufzeigen. Ich habe mich vorwiegend auf die EU-Zinssteuerrichtlinie, Informationsverbundsysteme und datenschutzrechtliche Fragestellungen sowie damit im Zusammenhang stehende grundrechtliche Bestimmungen konzentriert. Auch zurzeit in Diskussion stehende Reformen im Datenschutzrecht auf Unionsebene werden von mir besprochen. Da Vorgänge des Datenaustausches gerade im Finanzdienstleistungsbereich oft international stattfinden, habe ich einzelne Bereiche des internationalen Datenaustausches, vor allem das SWIFT-Abkommen, behandelt. Den internationalen Datenaustausch konnte ich jedoch nicht abschließend ausführen, da hierbei eine kaum überschaubare Zahl an Bestimmungen zu berücksichtigen wäre und auch sprachliche Grenzen bestehen.

Die Schlussfolgerungen am Ende meiner Arbeit sollen konkreten Handlungsbedarf zur weiteren Rechtsentwicklung aufzeigen.

Besonders bedanken möchte ich mich bei meinem Betreuer ao. Univ.-Prof. Dr. Christian Piska, der mir während der Arbeit an meiner Dissertation immer wieder verlässliche und hilfreiche Rückmeldungen gab, sowie auch bei o. Univ.-Prof. Dr. Bernhard Raschauer und ao. Univ.-Prof. Dr. Gerhard Muzak, die sich von Anfang bereit erklärt haben, die Dissertation nach den Bestimmungen des neuen Doktoratsstudienplans zu begutachten.

Auch meinen Eltern, ohne die das Studium nicht möglich gewesen wäre, möchte ich auf diesem Weg herzlich danken.

Inhaltsverzeichnis

VORWORT	III
INHALTSVERZEICHNIS.....	V
ABKÜRZUNGSVERZEICHNIS.....	IX
I. EINLEITUNG	1
II. BEGRIFFSBESTIMMUNGEN	3
A. DATENAUSTAUSCH.....	3
1. <i>Allgemeines zum Datenaustausch</i>	3
2. <i>Datenaustausch im österr DSG</i>	3
a) Allgemeines	3
b) Verwendung von Daten	4
c) Begriffsbestimmung.....	5
B. AUTOMATISCH	6
1. <i>Automationsunterstützt und manuell</i>	6
2. <i>Das Verbot automatisierter Einzelentscheidung</i>	7
C. FINANZDIENSTLEISTUNGEN	9
1. <i>Allgemeines</i>	9
2. <i>Finanzdienstleistung</i>	9
a) Fernabsatz-Finanzdienstleistungs-Richtlinie.....	9
b) Fern-Finanzdienstleistungs-Gesetz	10
(1) Definition.....	10
(2) Erläuterung der Definition	10
3. <i>Finanzdienstleister</i>	13
a) Finanzdienstleister	13
b) Auswahl sonstiger Finanzdienstleister	14
4. <i>Relevante Finanzdienstleistungen</i>	14
D. DIE EU-ZINSSTEUERRICHTLINIE	16
1. <i>Das Bankgeheimnis und die EU-Zinssteuerrichtlinie</i>	16
a) Das österreichische Bankgeheimnis.....	16
b) Die EU-Zinssteuerrichtlinie	17
c) Zusammenhang Bankgeheimnis – EU-Zinssteuerrichtlinie	18
(1) Allgemeines	18
(2) Das Bankgeheimnis und die EU-Zinssteuerrichtlinie	19
(3) Strukturelle Unterschiede = Bankgeheimnis?!.....	20
2. <i>Automatische Auskunftserteilung</i>	21
a) Begriff.....	21
(1) Art 8 der RL 2003/48/EG	21
(2) Art 9 der RL 2003/48/EG	21

b)	Ausnahmen von der automatischen Auskunftserteilung	22
c)	Höhe der Quellensteuer.....	23
d)	Beginn und Ende des Übergangszeitraumes	25
III.	AKTEURE IM ZUSAMMENHANG MIT DATENAUSTAUSCH	33
A.	BMF.....	33
B.	FMA	35
C.	OENB.....	38
D.	KREDITINSTITUTE UND ANDERE FINANZINSTITUTE	39
E.	DATENSCHUTZKOMMISSION UND DATENSCHUTZRAT	45
1.	<i>Allgemeines</i>	45
2.	<i>Datenschutzkommission</i>	45
a)	Grundzüge der Datenschutzkommission.....	45
b)	Urteil des EuGH und die Folgen für die DSK.....	51
(1)	Gesetzliche Änderungen.....	51
(2)	DSG-Novelle 2014 und die Verwaltungsgerichtsbarkeits-Novelle.....	53
3.	<i>Datenschutzrat</i>	56
a)	Geltende Rechtslage.....	56
b)	DSG-Novelle 2014.....	58
F.	SWIFT	60
IV.	INFORMATIONSVORBUNDENSYSTEME.....	63
A.	INFORMATIONSVORBUNDENSYSTEME IM BANKENBEREICH	63
1.	<i>Allgemeines</i>	63
2.	<i>Hoheitliches und nicht hoheitliches Handeln</i>	64
3.	<i>Anwendungsbereiche von Informationsverbundsystemen</i>	65
B.	ZENTRALES MELDEREGISTER	66
1.	<i>Begriff</i>	66
2.	<i>Beinhaltete Daten</i>	66
3.	<i>Zulässigkeit</i>	67
4.	<i>Judikatur der österr DSK</i>	68
5.	<i>Vergleichbare Systeme in Deutschland</i>	70
C.	WARNLISTE DER ÖSTERREICHISCHEN KREDITINSTITUTE.....	71
1.	<i>Begriff</i>	71
2.	<i>Beinhaltete Daten</i>	71
3.	<i>Zulässigkeit</i>	73
a)	Exkurs: Vorabkontrolle gem § 18 DSG	73
b)	Zulässigkeit der Warnliste	73
4.	<i>Judikatur der österr DSK</i>	75
5.	<i>Vergleichbare Systeme in Deutschland</i>	84
D.	KLEINKREDITEVIDENZ.....	86
1.	<i>Begriff</i>	86
2.	<i>Beinhaltete Daten</i>	86

3.	<i>Zulässigkeit</i>	86
4.	<i>Judikatur der österr DSK</i>	92
5.	<i>Vergleichbare Systeme in Deutschland</i>	92
E.	MOBILFUNKVERTRÄGE UND BONITÄTSDATENBANKEN	95
1.	<i>Begriff</i>	95
2.	<i>Beinhaltete Daten</i>	96
3.	<i>Zulässigkeit</i>	97
4.	<i>Judikatur der österr DSK</i>	99
5.	<i>Vergleichbare Systeme in Deutschland</i>	104
F.	EXKURS: BANK AGB 2000 – MEHRERE KLAUSELN UNWIRKSAM	106
1.	<i>AGB 1979</i>	106
2.	<i>„Neue“ Bank AGB 2000</i>	106
a)	<i>Entstehung</i>	106
b)	<i>Verfahren des VKI</i>	106
c)	<i>Urteil des OGH 4 Ob 179/02f</i>	107
(1)	<i>Z 26 der Bank AGB 2000</i>	107
(2)	<i>Z 27 der Bank AGB 2000</i>	110
V.	DATENSCHUTZRECHTLICHE HINTERGRÜNDE	113
A.	ÖSTERREICHISCHES DATENSCHUTZGESETZ (DSG)	113
1.	<i>Datenschutzrecht in Österreich</i>	113
2.	<i>Verwendung von Daten</i>	114
3.	<i>Datenverwendung in Österreich</i>	117
a)	<i>Allgemeines</i>	117
b)	<i>Verarbeitung</i>	118
c)	<i>Übermittlung</i>	127
d)	<i>Überlassung</i>	128
4.	<i>Datenübermittlung und -überlassung in MS des EWR</i>	128
a)	<i>Allgemeines</i>	128
b)	<i>Verwendung</i>	129
c)	<i>Übermittlung und Überlassung</i>	130
5.	<i>Datenübermittlung und -überlassung in „Drittstaaten“</i>	130
a)	<i>Allgemeines</i>	130
b)	<i>Angemessenes Datenschutzniveau</i>	133
c)	<i>Übermittlung und Überlassung</i>	137
d)	<i>Sonderbestimmungen im Bereich Finanzdienstleistungen</i>	143
B.	IM FINANZBEREICH RELEVANTE BESTIMMUNGEN	146
1.	<i>Verbraucherkreditrichtlinie</i>	146
2.	<i>Zahlungsdiensterichtlinie</i>	147
3.	<i>Geldwäschebestimmungen</i>	147
4.	<i>Elektronische Kommunikation</i>	148
5.	<i>Weitere zu beachtende Vorschriften und Mitteilungen</i>	149
6.	<i>SWIFT-Abkommen</i>	150

a)	Begriff.....	150
b)	Historische Entwicklung.....	151
c)	Inhalte des „SWIFT-Abkommens“.....	155
d)	Exkurs: Safe Harbor.....	160
C.	EDI UND SEPA	162
1.	<i>EDI – Elektronischer Datenaustausch</i>	162
2.	<i>SEPA – Single European Payment Area</i>	164
D.	BANKGEHEIMNIS UND DATENSCHUTZRECHT.....	166
1.	<i>Verhältnis von Bankgeheimnis und Datenschutzrecht</i>	166
2.	<i>Exkurs: Abkommen zwischen Österreich und Schweiz</i>	167
E.	REFORM DES „EUROPÄISCHEN DATENSCHUTZRECHTES“.....	171
VI.	GRUNDRECHTLICHE ANALYSE.....	177
A.	GRUNDRECHT AUF DATENSCHUTZ	177
1.	<i>§ 1 DSGVO</i>	177
2.	<i>Europäische Menschenrechtskonvention</i>	182
3.	<i>Charta der Grundrechte der Europäischen Union</i>	184
B.	DATENSCHUTZ UND TECHNIK.....	189
VII.	SCHLUSSFOLGERUNGEN.....	191
	LITERATURVERZEICHNIS	195
	VERWENDETE WEBSEITEN.....	205
	JUDIKATURVERZEICHNIS	207
	DEUTSCHE ZUSAMMENFASSUNG	211
	ENGLISH ABSTRACT.....	213
	LEBENS LAUF	215

Abkürzungsverzeichnis

Die Abkürzungen entsprechen den im Auftrag des Österreichischen Juristentages von *Friedl/Loebenstein* herausgegebenen Abkürzungs- und Zitierregeln der österreichischen Rechtssprache¹.

¹ *Friedl/Loebenstein*, Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen (AZR)⁷ (2012).

I. Einleitung

Im Rahmen des Studiums setzte ich mich in einem Seminar mit dem Bankgeheimnis auseinander. Ausgehend von dieser Thematik interessierten mich genauere Zusammenhänge und Hintergründe zu diesem Bereich. So stieß ich unter anderem auf die „automatische Auskunftserteilung“ in Art 9 der RL 2003/48/EG des Rates vom 3. Juni 2003 (EU-Zinssteuerrichtlinie).² Gem Art 10 Abs 1 der genannten RL müssen Belgien, Luxemburg und Österreich die Bestimmungen des Kapitels II (Auskunftserteilung) nicht anwenden, erhalten jedoch Auskünfte nach Kapitel II von anderen Mitgliedstaaten.

Im Rahmen meiner Dissertation möchte ich besonders auf diese Auskunftserteilung gegenüber anderen Mitgliedstaaten der Europäischen Union eingehen, vor allem unter dem Aspekt, wann bzw ob diese auch demnächst in Österreich Anwendung finden könnte.

Da diese Auskunftserteilung auch stets datenschutzrechtliche und grundrechtliche Aspekte berührt, habe ich als Titel den weiten Begriff des „Datenaustausches“ gewählt, den ich jedoch in der Folge anhand des österr DSG 2000 präzisieren werde. Um ein zu weitgehendes Thema zu vermeiden, findet sich im Titel die Einschränkung auf den Bereich der Finanzdienstleistungen, wenngleich ich feststellen konnte, dass es in diesem Bereich zahlreiche Anwendungen des (automatischen) Datenaustausches gibt. Auf die sehr bedeutsamen Informationsverbundsysteme werde ich etwa im vierten Kapitel näher eingehen. Ich hoffe, mit dieser Arbeit sowohl zur Klarheit in diesem Bereich beitragen zu können, als auch konkrete Vorschläge für notwendige legislative Änderungen geben zu können.

Soweit in meiner Dissertation personenbezogene Bezeichnungen nur in männlicher Form angeführt werden, beziehen sie sich auf Frauen und Männer in gleicher Weise.

² RL 2003/48/EG des Rates vom 3. Juni 2003 im Bereich der Besteuerung von Zinserträgen (ABl L 157 vom 26.06.2003, S 38); synonym für die EU-Zinssteuerrichtlinie werden auch die Bezeichnungen Sparzinsen-RL und Zinsen-RL verwendet.

II. Begriffsbestimmungen

A. Datenaustausch

1. Allgemeines zum Datenaustausch

Der Begriff „Datenaustausch“ ist ein rechtlich schwer fassbarer Begriff. Das österreichische DSG verwendet Begriffe wie „Verarbeitung“, „Übermittlung“ oder „Überlassung“ von Daten. Um in meiner Arbeit klare Begrifflichkeiten zu verwenden, möchte ich daher in diesem Kapitel eventuell unklare Begriffe klären und über Bestimmungen, die in der gesamten Arbeit immer wieder vorkommen werden, einen kurzen Überblick geben.

2. Datenaustausch im österr DSG

a) Allgemeines

Das DSG kennt keine explizite Regelung zum Datenaustausch. Die Terminologie des DSG definiert im ersten Abschnitt des zweiten Artikels unter anderem folgende Begriffe, die im Zusammenhang mit dem Datenaustausch stehen und deren Kenntnis daher von grundlegender Bedeutung für die noch zu besprechende Materie ist. Die Kenntnis folgender Begriffsdefinitionen ist daher unerlässlich:

- *Datenanwendung: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (§ 4 Z 8 DSG), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);³*
- *Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (§ 4 Z 9 DSG) als auch das Übermitteln (§ 4 Z 12 DSG) von Daten;⁴*
- *Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittels (Z 12) von Daten;⁵*

³ § 4 Z 7 DSG.

⁴ § 4 Z 8 DSG.

⁵ § 4 Z 9 DSG.

- *Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (vgl § 4 Z 5 DSG);⁶*
- *Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;⁷*

b) Verwendung von Daten

Sowohl das Verarbeiten als auch das Übermitteln von Daten definiert § 4 Z 8 DSG, wie soeben geschildert, als „Verwenden von Daten“. Die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses entspricht nach der Legaldefinition in § 4 Z 11 DSG dem Überlassen von Daten.

Als Überbegriff für die Handhabung von Daten wurde im österr DSG der Begriff „Verwenden“ eingeführt, der dem Begriff „Verarbeiten“ in der Datenschutzrichtlinie entspricht.⁸ Die Datenschutzrichtlinie unterscheidet jedoch nicht zwischen den im österr DSG gebräuchlichen Definitionen „Verarbeiten“ und „Übermitteln“.⁹

Unter „Verarbeiten“ iSd österr DSG wird jede Art der Handhabung der Daten mit Ausnahme des „Übermittels“ verstanden.¹⁰ „Übermitteln“ iSd DSG bezeichnet die Übergabe von Daten aus einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, wobei die Form dieser Weitergabe unerheblich ist.¹¹ Der zitierte Kommentar nennt hier etwa die Weitergabe in Form von EDV-Ausdrucken, auf elektronischem Weg, durch Auskunft, durch Publikation usw. Werden personenbezogene Daten eines Aufgabengebietes für ein anderes Aufgabengebiet verwendet, so handelt es sich ebenfalls um eine „Übermittlung“. Der Adressatenkreis entscheidet daher, ob es sich bei einem Datenaustausch um eine Übermittlung (Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister; auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers) oder eine Überlassung (Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen eines Auftragsverhältnisses)

⁶ § 4 Z 11 DSG.

⁷ § 4 Z 12 DSG.

⁸ *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Anm 9.

⁹ Vgl ebenda: *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Anm 9.

¹⁰ *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Anm 10.

¹¹ Vgl auch *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Anm 12.

handelt. Jede andere Art der Handhabung von Daten ist als „Verarbeiten“ von Daten einzuordnen.

Werden Daten durch den Auftraggeber an den Dienstleister oder auch umgekehrt weitergegeben, so handelt es sich nicht um eine Übermittlung iSd § 7 DSG, sondern um eine Überlassung, auf welche die Bestimmungen des § 7 leg cit keine Anwendung finden. Es müssen jedoch die Qualitätsgrundsätze gem § 6 DSG eingehalten werden.¹² Auf weitere Einzelheiten werde ich im fünften Kapitel genauer eingehen.¹³

c) Begriffsbestimmung

Um Unklarheiten zu vermeiden, bediene ich mich im Folgenden der Terminologie des DSG. Statt des Begriffes „Datenaustausch“ werde ich daher in dieser Arbeit die termini technici des DSG verwenden.

Zu betonen ist auch, dass sich das DSG nur auf personenbezogene Daten bezieht. Darunter sind Angaben über Betroffene zu verstehen, deren Identität bestimmt oder bestimmbar ist¹⁴ (direkt personenbezogene Daten). Indirekt personenbezogene Daten sind Daten, bei denen der Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.¹⁵

Bei der Definition in § 4 Z 1 DSG fällt auf, dass der Begriff „Daten“ mit dem Klammerausdruck „personenbezogene Daten“ umschrieben ist. Wenn somit im DSG der Begriff „Daten“ verwendet wird, handelt es sich stets um „personenbezogene Daten“.¹⁶ Vom Begriff der „Person“ werden im österr DSG auch „juristische“ Personen erfasst. Fraglich ist, ob auch ein einzelnes „Datum“ vom Schutz des Datenschutzgesetzes umfasst ist, da stets das Plural „Daten“ verwendet wird. In Anschluss an *Jahnel*, der wiederum auf *Duschanek* verweist¹⁷, ist entgegen dem Wortlaut anzunehmen, dass auch ein einzelnes Datum geschützt wird. Es wäre nicht nachvollziehbar, warum nur mehrere Daten geschützt sein sollen, da auch schon die Missachtung des Schutzes eines einzelnen personenbezogenen Datums gravierende Auswirkungen für ein Individuum haben kann.

¹² Vgl auch *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Anm 11.

¹³ Siehe V Datenschutzrechtliche Hintergründe.

¹⁴ § 4 Z 1 DSG.

¹⁵ Vgl *Jahnel*, Handbuch Datenschutzrecht, 3/78.

¹⁶ Vgl *Jahnel*, Handbuch Datenschutzrecht, 3/71.

¹⁷ *Jahnel*, Handbuch Datenschutzrecht, 3/71 mit Verweis auf *Duschanek*, § 1 DSG 2000, Rz 25, S 20 f.

B. Automatisch

In diesem Abschnitt möchte ich „automatisch“ genauer definieren. Dieser Begriff wird auch im Alltag des Öfteren verwendet. Im Bereich des Datenschutzgesetzes findet sich vor allem das Gegensatzpaar „automationsunterstützt“ und „manuell“, womit das Gegenteil von automationsunterstützt gemeint ist.

1. Automationsunterstützt und manuell

§ 1 Abs 3 DSG definiert, dass jedermann nach Maßgabe gesetzlicher Bestimmungen gewisse Rechte¹⁸ hat. Diese bestehen hinsichtlich personenbezogener Daten sowohl bei *automationsunterstützter* Verwendung, als auch bei *manuell* geführten Dateien. Manuell wird hierbei als „ohne Automationsunterstützung“ umschrieben.

§ 2 Abs 1 DSG normiert, dass die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im *automationsunterstützten* Datenverkehr Bundessache ist.

§ 4 Z 7 DSG definiert ua die *automationsunterstützte* Datenanwendung und umschreibt *automationsunterstützt* mit „maschinell und programmgesteuert“¹⁹. Auch weitere Bestimmungen des DSG verwenden den Begriff *automationsunterstützt*²⁰.

Im Zusammenhang mit dem „automatischen Informationsaustausch“ regelt Art 9 der RL 2003/48/EG, dass die Auskünfte über sämtliche während eines Steuerjahres erfolgten Zinszahlungen mindestens einmal jährlich *automatisch* erteilt werden, und zwar binnen sechs Monaten nach dem Ende des Steuerjahres des Mitgliedstaats, in dem die Zahlstelle niedergelassen ist. Somit wird mit *automatisch* darauf abgestellt, dass die Auskünfte ohne neuerliche Aufforderung zu erteilen sind. Die Erteilung wird wohl zumindest maschinell erfolgen. Inwiefern jedoch ein Programm die Weitergabe der Informationen abwickelt bzw wie dieser Austausch konkret abläuft, ist in dieser Bestimmung nicht genauer umschrieben.

Konkret meldet beim *automatischen* Informationsaustausch die Zahlstelle, zB ein deutsches Kreditinstitut, der nationalen Steuerbehörde die gem Art 8 der RL 2003/48/EG zu erteilenden

¹⁸ Auskunftsrecht (Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden – vgl § 1 Abs 3 Z 1 DSG), Richtigstellungsrecht unrichtiger Daten (vgl § 1 Abs 3 Z 2 DSG) und Lösungsrecht unzulässigerweise verarbeiteter Daten (vgl § 1 Abs 3 Z 2 DSG).

¹⁹ Vgl § 4 Z 7 DSG.

²⁰ Vgl §§ 20 und 21 zur automationsunterstützten Prüfung von Meldungen von Datenanwendungen; § 27 Abs 6 über automationsunterstützt lesbare Datenträger; § 49 zur automatisierten Einzelentscheidung; § 50a Abs 7 zum Verbot des automationsunterstützten Bilddatenabgleichs; § 58 zu manuell geführten Dateien und § 61 Abs 5, der eine Übergangsregelung enthält.

Auskünfte. Die nationale Steuerbehörde gibt sodann diese Daten an den Ansässigkeitsstaat des wirtschaftlichen Eigentümers weiter.

So meldet etwa die deutsche Bank die Identität und den Wohnsitz des gemäß Art 3 der RL festgestellten wirtschaftlichen Eigentümers, der etwa in Österreich ansässig ist, sowie Name und Anschrift der deutschen Bank, Kontonummer des wirtschaftlichen Eigentümers oder, in Ermangelung einer solchen, Kennzeichen der Forderung, aus der die Zinsen herrühren, und weitere Auskünfte zur Zinszahlung an die deutsche Finanzbehörde. Diese meldet diese Auskünfte weiter an die österreichische Finanzbehörde, die dann überprüfen kann, ob die in Deutschland bezogenen Zinsen, in Österreich versteuert wurden. Umgekehrt erfolgt bei in anderen Mitgliedstaaten ansässigen Personen in Österreich jedoch nur ein Quellensteuerabzug. Nach einem Verteilungsschlüssel²¹ wird dann die Quellensteuer an zB die Bundesrepublik Deutschland überwiesen.²²

2. Das Verbot automatisierter Einzelentscheidung

Gemäß § 49 Abs 1 DSGVO darf niemand einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht. Genannt werden beispielsweise die Bewertung seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.²³

Abs 2 *leg cit* bietet jedoch weitgehende Ausnahmemöglichkeiten und erlaubt eine ausschließlich automationsunterstützt erzeugte Entscheidung, wenn dies gesetzlich ausdrücklich vorgesehen ist oder die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluss oder Erfüllung des Vertrages stattgegeben wurde oder die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen – beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen, – garantiert wird.²⁴

²¹ Vgl II.D.1.c)(1) Allgemeines.

²² Vgl auch das Video des Schweizer Fernsehens zum Automatischen Informationsaustausch: <http://www.videoportal.sf.tv/video?id=78d4ac1c-1116-437c-97d7-5bd43baa62a7> (Stand: 18.08.2013).

²³ Vgl § 49 Abs 1 DSGVO.

²⁴ Vgl § 49 Abs 2 DSGVO.

§ 49 Abs 3 DSGVO definiert das Recht auf Darlegung des logischen Ablaufes der automatisierten Entscheidungsfindung im Zusammenhang mit automatisierten Einzelentscheidungen, wobei die Bestimmung zum Auskunftsrecht²⁵ sinngemäß gilt.²⁶

²⁵ § 26 DSGVO, verwiesen wird auf die Absätze 2 bis 10.

²⁶ Vgl auch die Beschwerdemöglichkeit in § 31 Abs 1 DSGVO.

C. Finanzdienstleistungen

1. Allgemeines

Den Begriff „Finanzdienstleistungen“ verwende ich in Abgrenzung zu anderen Bereichen, in denen der Datenschutz von großer Bedeutung ist (zB Arbeitsrecht, Krankenversicherungsrecht etc). Wie die folgende Auseinandersetzung mit diesem Begriff zeigen wird, umfasst der Begriff der Finanzdienstleistungen ein weites Feld, wobei ich mich im Rahmen dieser Dissertation nicht abschließend mit allen Bereichen detailliert auseinandersetzen werde können; der Schwerpunkt liegt im Bereich des automatischen Datenaustausches im Bereich der Finanzdienstleistungen.

2. Finanzdienstleistung

Der Begriff der Finanzdienstleistung wurde in Österreich aufgrund einer Europäischen Richtlinie im Fern-Finanzdienstleistungs-Gesetz umgesetzt²⁷. Im Folgenden möchte ich die Bestimmungen kurz vergleichen:

a) Fernabsatz-Finanzdienstleistungs-Richtlinie

Im Sinn der Fernabsatz-Finanzdienstleistungs-Richtlinie²⁸ bezeichnet der Ausdruck „Finanzdienstleistung“ gem Art 2 lit b:

b) (...) jede Bankdienstleistung sowie jede Dienstleistung im Zusammenhang mit einer Kreditgewährung, Versicherung, Altersversorgung von Einzelpersonen, Geldanlage oder Zahlung;

Die Definition in der Fernabsatz-Finanzdienstleistungs-Richtlinie ist eine umfassende und beinhaltet neben der Bankdienstleistung jede Dienstleistung, die im Zusammenhang mit einer Kreditgewährung, Versicherung, Altersversorgung von Einzelpersonen, einer Geldanlage oder einer Zahlung steht. Diese weitgehende Definition findet sich ebenso im österr Fern-Finanzdienstleistungs-Gesetz.

²⁷ Vgl auch *Reimer in Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 550.

²⁸ Richtlinie 2002/65/EG des Europäischen Parlaments und des Rates vom 23. September 2002 über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG (ABl L 271 vom 09.10.2002, S 16-24).

b) Fern-Finanzdienstleistungs-Gesetz

(1) Definition

In Art 1 § 3 Abs 2 Fern-Finanzdienstleistungs-Gesetz²⁹ findet sich folgende Definition:

§ 3 Abs 2 Z 2: Finanzdienstleistung: jede Bankdienstleistung sowie jede Dienstleistung im Zusammenhang mit einer Kreditgewährung, Versicherung, Altersversorgung von Einzelpersonen, Geldanlage oder Zahlung;

Die Definition der Fernabsatz-Finanzdienstleistungs-Richtlinie wurde daher in Österreich wortgleich übernommen.

Die Gesetzesmaterialien erwähnen, dass die Begriffe in § 3 FernFinG großteils schon dem allgemeinen Fernabsatzrecht (§§ 5a ff KSchG) bekannt sind. Die Definition der „Finanzdienstleistung“ in dem am 27. Mai 2004 im Nationalrat beschlossenen Fern-Finanzdienstleistungs-Gesetz ist jedoch neu³⁰.

(2) Erläuterung der Definition

Was ist davon aus österreichischer Sicht erfasst?

Gemäß den Gesetzesmaterialien sind von der Definition in § 3 Abs 2 FernFinG aus österreichischer Sicht jedenfalls Bankgeschäfte im Sinn des § 1 Abs 1 BWG erfasst. Auch fallen alle Arten von Versicherungsverträgen, Pensionsverträgen, Anlagegeschäften und Zahlungsdienstleistungen darunter. Hierzu gehören nach den Gesetzesmaterialien auch Dienstleistungen im Zusammenhang mit Devisen, Geldmarktinstrumenten, handelbaren Wertpapieren, Anteilen an Anlagegesellschaften, Finanz- und Zinstermingeschäften, Swaps und Optionen.

Weiter Anwendungsbereich:

„Der Anwendungsbereich umfasst daher höchst unterschiedliche Dienstleistungen, von reinen Finanzmarkttransaktionen bis hin zu Hypothekarkrediten, von Reisegepäckversicherungen bis zum Abschluss eines Kreditkartenvertrags. Es sind auch nicht nur <Dienstleistungen> im

²⁹ BGBl I Nr 62/2004, zuletzt geändert durch BGBl Nr 66/2009: Bundesgesetz, mit dem ein Bundesgesetz über den Fernabsatz von Finanzdienstleistungen an Verbraucher (Fern-Finanzdienstleistungs-Gesetz - FernFinG) erlassen wird und das Konsumentenschutzgesetz, das Versicherungsvertragsgesetz sowie das Wertpapieraufsichtsgesetz geändert werden.

³⁰ 467 d.B. der XXII. GP - Fern-Finanzdienstleistungs-Gesetz: Besonderer Teil der Erläuterungen in den Gesetzesmaterialien, zu § 3.

engen Wortsinn, sondern beispielsweise auch der Kauf von Wertpapieren oder das Finanzierungsleasing erfasst.“³¹

Vergleich mit anderen Sprachfassungen - Einschränkung:

Bei der Auslegung europäischer Rechtsakte sind stets auch die anderen Sprachfassungen zu beachten. Die Gesetzesmaterialien verweisen besonders auf die anderen Sprachfassungen zur Formulierung „Dienstleistung im Zusammenhang mit (...)“. Nach den bibliographischen Angaben zur RL 2002/65/EG auf der Webseite <http://eur-lex.europa.eu> ist die RL in allen Amtsprachen der Europäischen Union und zusätzlich in Isländisch und Norwegisch verbindlich.³² Aufgrund meiner persönlichen Sprachkompetenz durch Auslandsaufenthalte in Frankreich und Großbritannien, möchte ich mich auf einen detaillierten Vergleich der deutschen, englischen und französischen Sprachfassungen beschränken.

Die deutsche Sprachfassung zur Definition des Ausdrucks „Finanzdienstleistung“ lautet „jede Bankdienstleistung sowie jede Dienstleistung im Zusammenhang mit einer Kreditgewährung, Versicherung, Altersversorgung von Einzelpersonen, Geldanlage oder Zahlung“³³;

In der englischen Sprachfassung findet sich folgende Definition für “financial service”: “any service of a banking, credit, insurance, personal pension, investment or payment nature”.

Die französische Sprachfassung beschreibt „service financier“ folgendermaßen: „tout service ayant trait à la banque, au crédit, à l'assurance, aux retraites individuelles, aux investissements et aux paiements“.

Die Gesetzesmaterialien betonen, dass die Dienstleistung nicht nur irgendeinen Zusammenhang mit einer Kreditgewährung, Versicherung oder Ähnlichem aufweisen muss, sondern dass die Dienstleistung selbst die entscheidenden Wesensmerkmale eines der genannten Vertragsinhalte haben muss.

³¹ 467 d.B. der XXII. GP - Fern-Finanzdienstleistungs-Gesetz: Besonderer Teil der Erläuterungen in den Gesetzesmaterialien, zu § 3.

³² Die RL 2002/65/EG gilt durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr 47/2003 vom 16. Mai 2003 zur Änderung des Anhangs IX (Finanzdienstleistungen) und des Anhangs XIX (Verbraucherschutz) des EWR-Abkommens auch für den Europäischen Wirtschaftsraum (EWR), der neben den Mitgliedstaaten der Europäischen Union folgende Staaten umfasst: Island, Liechtenstein und Norwegen.

³³ Art 2 lit b der RL 2002/65/EG; vgl auch weiter oben.

Ich möchte daher die Bedeutung der Formulierung „im Zusammenhang“ erörtern und darlegen, ob es sich um irgendeinen Zusammenhang handelt, oder ob die Dienstleistung selbst die entscheidenden Wesensmerkmale eines der genannten Vertragsinhalte zu beinhalten hat.

Die englische Sprachfassung spricht von „service of a banking, credit, insurance, personal pension, investment or payment nature“. Es handelt sich somit wörtlich übersetzt um eine Dienstleistung, die durch folgende Bereiche charakterisiert (arg: „of a ... nature“) ist: Bank-, Kredit- und Versicherungsgeschäft, sowie Altersversorgung von Einzelpersonen, Geldanlage oder Zahlung.

Die französische Sprachfassung ist ähnlich zu interpretieren, da die Formulierung „tout service ayant trait à (...)“ auch auf das Wesensmerkmal der Dienstleistung anspielt. „Trait“ könnte sowohl ein Substantiv, als auch ein abgewandeltes Verb darstellen³⁴. Da „traire“ übersetzt „melken“ heißt, ist in diesem Zusammenhang davon auszugehen, dass „trait“ in der gegebenen Formulierung ein Substantiv darstellt und als solches mit „Charakterzug“ oder „Merkmal“ übersetzt werden sollte. Die Kombination „avoir trait à (+ acc)“ bedeutet laut Wörterbüchern „sich beziehen auf“ oder „Bezug haben auf“.

Es werden dadurch alle Dienstleistungen miteinbezogen, die ein bestimmtes Wesensmerkmal („trait“) haben („ayant“). Bei „ayant“ handelt es sich um das Participe présent von „avoir“ (Grundform von „haben“), wobei das Participe présent auf Deutsch nicht wörtlich übersetzt werden kann, da es im Französischen als Sonderform zur Verkürzung von Sätzen verwendet wird. Auf Deutsch könnte die Phrase wohl am besten durch einen separaten Relativsatz übersetzt werden mit „alle Dienstleistungen, die zum Wesensmerkmal ein Bank-, Kredit-, Versicherungsgeschäft (...) haben“ oder „alle Dienstleistungen, die sich auf ein Bank-, Kredit-, Versicherungsgeschäft (...) beziehen“.

Der Vergleich mit den anderen Sprachfassungen führt daher zum klaren Schluss, dass es sich nicht um irgendeinen Zusammenhang handeln kann, sondern dass es sich dann um eine Finanzdienstleistung handelt, wenn die Dienstleistung durch die Kreditgewährung, Versicherung, Altersversorgung von Einzelpersonen, Geldanlage oder Zahlung charakterisiert ist und somit ein Wesensmerkmal der Dienstleistung darstellt. Diese notwendige Charakterisierung der Dienstleistung kommt im Vergleich zur deutschen Sprachfassung auf Englisch und Französisch besser zur Geltung, da dort mehr Betonung auf das

³⁴ Die dritte Person Einzahl von „traire“ lautet „trait“.

Wesensmerkmal der Dienstleistung gelegt wird und nicht ein bloßer „Zusammenhang“ erforderlich ist.

Weitere einschränkende Auslegung:

Abschließend zu § 3 FernFinG betonen die Gesetzesmaterialien auch die restriktive Auslegung der „Dienstleistungen im Zusammenhang mit einer Zahlung“. Darunter sind somit Verträge zu verstehen, bei denen der Unternehmer den Verbraucher bei von diesem zu leistenden Zahlungen durch Dienstleistungen unterstützt oder sich dazu verpflichtet. Beispiele hierfür³⁵ sind etwa der Abschluss eines Kreditkartenvertrags, die Vereinbarung mit der Bank, dass diese dem Kunden eine Zahlungskarte ausstellt, mit der er elektronisch Zahlungen leisten kann, die dann von seinem Konto abgebucht werden, oder auch die Vereinbarung zwischen einem Telefonnetzbetreiber und seinem Kunden, dass der Netzbetreiber dem Kunden Entgelte für Leistungen Dritter, die der Kunde über das Telefonnetz in Anspruch nimmt, mit der monatlichen Telefonrechnung in Rechnung stellt und in der Folge an den Dritten weiterleitet. Bloße Kaufverträge, bei denen eine „Zahlung“ zu leisten ist, sind nicht schon deshalb vom Begriff der Finanzdienstleistung erfasst.

3. Finanzdienstleister

Als Finanzdienstleister können jene bezeichnet werden, die Finanzdienstleistungen ausführen. *Raschauer* unterscheidet hierbei zwischen Finanzdienstleistern und sonstigen Finanzdienstleistern³⁶.

a) Finanzdienstleister

„Finanzdienstleister bieten gewerbsmäßig Dienstleistungen auf dem Finanzmarkt an“³⁷. *Raschauer* nennt für den Bereich des „geregelten Marktes“ insb die Börsen, geregelt im BörseG³⁸. Weiters zählt er hierzu die Kreditinstitute (vgl BWG³⁹) und die Zahlungsinstitute (vgl ZaDiG⁴⁰). Zum Teil fallen auch die Versicherungsunternehmen (vgl VAG⁴¹) darunter.

³⁵ Vgl ebenso 467 d.B. der XXII. GP - Fern-Finanzdienstleistungs-Gesetz: Besonderer Teil der Erläuterungen in den Gesetzesmaterialien, zu § 3.

³⁶ Vgl *Raschauer*, Bankenaufsicht (Skriptum)⁸ (2012) 91.

³⁷ *Raschauer*, Bankenaufsicht (Skriptum)⁸ (2012) 91.

³⁸ BGBl I Nr 555/1989, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz vom 8. November 1989 über die Wertpapier- und allgemeinen Warenbörsen und über die Abänderung des Börsensensale-Gesetzes 1949 und der Börsegesetz-Novelle 1903 (Börsegesetz 1989 - BörseG).

³⁹ BGBl I Nr 532/1993, zuletzt geändert durch BGBl I Nr 135/2013: Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG), über Kapitalanlagefonds (Investmentfondsgesetz - InvFG 1993), über Bausparkassen (Bausparkassengesetz - BSpG), über die Aufhebung des Kreditwesengesetzes, der Artikel II und III des Bundesgesetzes BGBl Nr 325/1986, des Bankagentengesetzes, des Geldinstitutezentralegesetzes, des Bundesgesetzes über die Geschäftsaufsicht, des Rekonstruktionsgesetzes, des Bundesgesetzes betreffend den

b) Auswahl sonstiger Finanzdienstleister

Raschauer gibt weiters einen nicht abschließenden Überblick über sonstige Finanzdienstleister und nennt auch den jeweiligen zu beachtenden Regelungsbereich⁴²:

- Leasingunternehmen (GewO⁴³),
- Wertpapierfirmen / Wertpapierdienstleistungsunternehmen: Anlageberatung, Portfolioverwaltung (WAG⁴⁴),
- Rating-Agenturen (EG-VO⁴⁵),
- Finanzanalysten (BörseG, WAG),
- vertraglich gebundene Vermittler (§ 136a GewO, WAG),
- gewerbliche Vermögensberater (§ 136a GewO),
- Versicherungsvermittler (§ 136b GewO) und
- Wertpapiervermittler (reglementiertes Gewerbe).

4. Relevante Finanzdienstleistungen

In meiner Dissertation werde ich mich weniger mit den sonstigen Finanzdienstleistungen beschäftigen und dafür besonders auf die Bankdienstleistungen sowie jede Dienstleistung im Zusammenhang mit einer Kreditgewährung oder Geldanlage eingehen. Inwieweit Daten bei

Verkauf von Aktien verstaatlichter Banken, von Teilen des Bundesgesetzes über die Neuordnung des Kindschaftsrechts, des Bundesgesetzes über Kapitalanlagefonds (Investmentfondsgesetz), des Versicherungsaufsichtsgesetzes 1931, der Einführungsverordnung zum Versicherungsaufsichtsgesetz 1931 und über die Änderung des Bundes-Verfassungsgesetzes in der Fassung von 1929, des Sparkassengesetzes, des Hypothekenbankgesetzes, des Pfandbriefgesetzes, der Einführungsverordnung zum Hypothekenbank- und zum Pfandbriefgesetz, des Beteiligungsfondsgesetzes, des Postsparkassengesetzes 1969, des Kapitalmarktgesetzes, des Versicherungsaufsichtsgesetzes 1978, des Prämienparförderungsgesetzes, des Körperschaftsteuergesetzes 1988, des Bewertungsgesetzes, der Gewerbeordnung 1973 und des Rechnungslegungsgesetzes (Finanzmarktanpassungsgesetz 1993).

⁴⁰ BGBl I Nr 66/2009, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz, mit dem ein Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG) erlassen und das Bankwesengesetz, das Fern-Finanzdienstleistungs-Gesetz, das Konsumentenschutzgesetz, das Finanzmarktaufsichtsbehördengesetz, das Versicherungsaufsichtsgesetz und das Wertpapieraufsichtsgesetz 2007 geändert werden sowie das Überweisungs-gesetz aufgehoben wird.

⁴¹ BGBl Nr 569/1978, zuletzt geändert durch BGBl I Nr 83/2013: Bundesgesetz vom 18. Oktober 1978 über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz - VAG).

⁴² *Raschauer*, Bankenaufsicht (Skriptum)⁸ (2012) 91.

⁴³ BGBl Nr 194/1994, zuletzt geändert durch BGBl I Nr 125/2013: Gewerbeordnung 1994 (GewO 1994).

⁴⁴ BGBl I Nr 60/2007, zuletzt geändert durch BGBl I Nr 135/2013: Bundesgesetz, mit dem ein Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007) erlassen wird sowie das Bankwesengesetz, das Börsegesetz 1989, das Investmentfondsgesetz, das Kapitalmarktgesetz, das Finanzmarktaufsichtsbehördengesetz, das Konsumentenschutzgesetz und die Gewerbeordnung 1994 geändert werden.

⁴⁵ Verordnung (EG) Nr 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen (ABl L 302 vom 17.11.2009, S 1–31), deren deutsche Sprachfassung bereits zwei Mal berichtigt wurde.

Dienstleistungen im Zusammenhang mit Versicherungen, Altersversorgung von Einzelpersonen oder Zahlungen verwendet oder überlassen werden dürfen, werde ich nur teilweise ansprechen.

D. Die EU-Zinssteuerrichtlinie

Ergänzend zu den Begriffsbestimmungen des Titels meiner Dissertation⁴⁶ gebe ich bewusst in einem weiteren Teil des zweiten Kapitels einen Überblick über die „EU-Zinssteuerrichtlinie“ und das österreichische Bankgeheimnis. Dies soll dazu dienen, die Zusammenhänge zwischen den österreichischen Bestimmungen und den europarechtlichen Vorgaben der EU-Zinssteuerrichtlinie klar darzulegen. Somit sollen einzelne später aufkommende Fragen systematisch eingeordnet werden können.

1. Das Bankgeheimnis und die EU-Zinssteuerrichtlinie

a) Das österreichische Bankgeheimnis

Das österreichische Bankgeheimnis ist in § 38 BWG⁴⁷ normiert. Darin heißt es:

§ 38 (1) Kreditinstitute, ihre Gesellschafter, Organmitglieder, Beschäftigte sowie sonst für Kreditinstitute tätige Personen dürfen Geheimnisse, die ihnen ausschließlich auf Grund der Geschäftsverbindungen mit Kunden oder auf Grund des § 75 Abs 3 anvertraut oder zugänglich gemacht worden sind, nicht offenbaren oder verwerten (Bankgeheimnis). Werden Organen von Behörden sowie der Österreichischen Nationalbank bei ihrer dienstlichen Tätigkeit Tatsachen bekannt, die dem Bankgeheimnis unterliegen, so haben sie das Bankgeheimnis als Amtsgeheimnis zu wahren, von dem sie nur in den Fällen des Abs 2 entbunden werden dürfen. Die Geheimhaltungsverpflichtung gilt zeitlich unbegrenzt.

(2) Die Verpflichtung zur Wahrung des Bankgeheimnisses besteht nicht

- 1. im Zusammenhang mit einem Strafverfahren auf Grund einer gerichtlichen Bewilligung (§ 116 StPO) gegenüber den Staatsanwaltschaften und Strafgerichten und mit eingeleiteten Strafverfahren wegen vorsätzlicher Finanzvergehen, ausgenommen Finanzordnungswidrigkeiten, gegenüber den Finanzstrafbehörden;*
- 2. im Falle der Verpflichtung zur Auskunftserteilung nach § 41 Abs 1 und 2, § 61 Abs 1, § 93 und § 93a;*
- 3. im Falle des Todes des Kunden gegenüber dem Abhandlungsgericht und Gerichtskommissär;*
- 4. wenn der Kunde minderjährig oder sonst pflegebefohlen ist, gegenüber dem Vormundschafts- oder Pflegschaftsgericht;*
- 5. wenn der Kunde der Offenbarung des Geheimnisses ausdrücklich und schriftlich zustimmt;*
- 6. für allgemein gehaltene bankübliche Auskünfte über die wirtschaftliche Lage eines Unternehmens, wenn dieses der Auskunftserteilung nicht ausdrücklich widerspricht;*
- 7. soweit die Offenbarung zur Klärung von Rechtsangelegenheiten aus dem Verhältnis zwischen Kreditinstitut und Kunden erforderlich ist;*

⁴⁶ Automatischer (vgl oben II.B) Datenaustausch (vgl oben II.A) im Bereich der Finanzdienstleistungen (vgl oben II.C).

⁴⁷ BGBl Nr 532/1993, zuletzt geändert durch BGBl I Nr 135/2013.

8. hinsichtlich der Meldepflicht des § 25 Abs 1 des Erbschafts- und Schenkungssteuergesetzes;

9. im Fall der Verpflichtung zur Auskunftserteilung an die FMA gemäß dem WAG und dem BörseG.

(3) Ein Kreditinstitut kann sich auf das Bankgeheimnis insoweit nicht berufen, als die Offenbarung des Geheimnisses zur Feststellung seiner eigenen Abgabepflicht erforderlich ist.

(4) Die Bestimmungen der Abs 1 bis 3 gelten auch für Finanzinstitute und Unternehmen der Vertragsversicherung bezüglich § 75 Abs 3 und für Sicherungseinrichtungen, ausgenommen die gemäß den §§ 93 bis 93b erforderliche Zusammenarbeit mit anderen Sicherungssystemen sowie Einlagensicherungseinrichtungen und Anlegerentschädigungssystemen.

(5) (Verfassungsbestimmung) Die Abs 1 bis 4 können vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Abgeordneten und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen abgeändert werden.

Auf nähere Zusammenhänge, insbesondere die Ausnahmebestimmung des Abs 2 leg cit, werde ich an späterer Stelle noch genauer eingehen.

b) Die EU-Zinssteuerrichtlinie

Die EU-Zinssteuerrichtlinie⁴⁸ wurde vom Rat der Europäischen Union 2003 beschlossen, eine Grundsatzeinigung wurde am 21. Jänner 2003 erreicht⁴⁹, wobei dem Rat bereits im Juni 1998 von der Europäischen Kommission ein Entwurf vorgelegt wurde.⁵⁰ In der Richtlinie werden Regelungen normiert, die letztlich ein Ziel verfolgen: „Erträge, die in einem Mitgliedstaat im Wege von Zinszahlungen an wirtschaftliche Eigentümer, die natürliche Personen sind und die in einem anderen Mitgliedstaat steuerlich ansässig sind, erzielt werden,“⁵¹ sollen nach den Rechtsvorschriften dieses letzteren Mitgliedstaats effektiv besteuert werden.⁵²

Gem Art 10 Abs 1 der RL 2003/48/EG gilt für Belgien, Luxemburg und Österreich ein Übergangszeitraum, während dem die Bestimmungen des Kapitels II (Auskunftserteilung) nicht angewendet werden. Um dennoch eine effektive Mindestbesteuerung von Erträgen, „die in einem Mitgliedstaat im Wege von Zinszahlungen an wirtschaftliche Eigentümer, die

⁴⁸ RL 2003/48/EG des Rates vom 3. Juni 2003 im Bereich der Besteuerung von Zinserträgen (ABl L 157 vom 26.06.2003, S 38-48); synonym für die EU-Zinssteuerrichtlinie werden auch die Bezeichnungen Sparzinsen-RL und Zinsen-RL verwendet.

⁴⁹ Vgl *Urlesberger*, *Europarecht: Das Neueste auf einen Blick*, wbl 2003, 118 (118) mit Verweis auf MEMO/03/13 vom 22.01.2003.

⁵⁰ *Heidenbauer*, *Internationale Aspekte der EU-Quellensteuer*, SWI 2006, 459.

⁵¹ Art 1 Abs 1 der RL 2003/48/EG.

⁵² Vgl Art 1 Abs 1 der RL 2003/48/EG und der 8. Erwägungsgrund der RL 2003/48/EG sowie *Aigner*, *Habilitationsschrift: Die SparzinsenRL – Koordinierung der Besteuerung von Zinsen in Europa*, taxlex 2009, 540 (541).

natürliche Personen und in einem anderen Mitgliedstaat steuerlich ansässig sind“⁵³, zu gewährleisten, erheben Belgien, Luxemburg und Österreich während des Übergangszeitraumes eine Quellensteuer, deren Höhe bis auf 35 % der Zinsen ansteigt. Die Richtlinie wurde in Österreich durch das EU-Quellensteuergesetz⁵⁴ umgesetzt.

Die Richtlinie 77/799/EWG des Rates vom 19. Dezember 1977 über die Amtshilfe der zuständigen Behörden der Mitgliedstaaten im Bereich der direkten und indirekten Steuern⁵⁵ sollte in Ergänzung zur RL 2003/48/EG weiterhin angewandt werden, soweit die RL 2003/48/EG nichts anderes bestimmt, da sie den Mitgliedstaaten bereits eine Grundlage für die zu steuerlichen Zwecken erfolgende gegenseitige Auskunftserteilung über die von der vorliegenden Richtlinie erfassten Einkommen bietet.⁵⁶

Der in der RL 2003/48/EG vorgesehene automatische Austausch von Auskünften zwischen den Mitgliedstaaten über die von dieser Richtlinie erfassten Zinszahlungen ermöglicht eine effektive Besteuerung dieser Zinszahlungen in dem Mitgliedstaat, in dem der wirtschaftliche Eigentümer steuerlich ansässig ist, entsprechend den nationalen Rechtsvorschriften dieses Staates. Auf die in Art 8 der RL 77/799/EWG niedergelegten Grenzen des Auskunftsaustauschs können sich daher jene Mitgliedstaaten nicht berufen, die Auskünfte nach dieser Richtlinie austauschen.⁵⁷

c) Zusammenhang Bankgeheimnis – EU-Zinssteuerrichtlinie

(1) Allgemeines

Im 17. Erwägungsgrund der RL 2003/48/EG werden als Grund für den Übergangszeitraum im Bereich der automatischen Auskunftserteilung „strukturelle Unterschiede“⁵⁸ genannt. Durch die Erhebung einer Quellensteuer, deren Steuersatz schrittweise auf 35 % angehoben werde, könne aber ein Minimum an effektiver Besteuerung sichergestellt werden.⁵⁹ Der größere Teil der Einnahmen aus der Quellensteuer – in Österreich sind es gem § 9 Abs 2 EU-QuStG drei Viertel (= 75 %) des Steueraufkommens – sollte von Belgien, Luxemburg und Österreich an

⁵³ Vgl Art 10 Abs 1 der RL 2003/48/EG.

⁵⁴ BGBl I Nr 33/2004, zuletzt geändert durch BGBl I Nr 135/2013: Bundesgesetz, mit dem das Bundesgesetz zur Durchführung der Richtlinie der Europäischen Gemeinschaften über die gegenseitige Amtshilfe im Bereich der direkten und indirekten Steuern (EG-Amtshilfegesetz - EG-AHG) geändert wird und ein EU-Quellensteuergesetz (EU-QuStG) erlassen wird.

⁵⁵ Richtlinie 77/799/EWG des Rates vom 19. Dezember 1977 über die gegenseitige Amtshilfe zwischen den zuständigen Behörden der Mitgliedstaaten im Bereich der direkten Steuern (ABl L 336 vom 27.12.1977, S 15–20).

⁵⁶ Vgl 15. Erwägungsgrund der RL 2003/48/EG.

⁵⁷ Vgl 16. Erwägungsgrund der RL 2003/48/EG.

⁵⁸ Vgl 17. Erwägungsgrund der RL 2003/48/EG.

⁵⁹ Ebenso im 17. Erwägungsgrund der RL 2003/48/EG.

den jeweiligen Wohnsitzmitgliedstaat des wirtschaftlichen Eigentümers der Zinsen weitergeleitet werden.⁶⁰

(2) Das Bankgeheimnis und die EU-Zinssteuerrichtlinie

Im Besonderen Teil der Gesetzesmaterialien zur Regierungsvorlage⁶¹ heißt es: „Wenn die Einrichtung weder zur Behandlung als OGAW [Organismus für gemeinsame Anlagen in Wertpapieren] optiert, noch auf das Bankgeheimnis verzichtet hat, ist ein Quellensteuerabzug vorgesehen. Dieser Quellensteuerabzug entspricht dem Artikel 11 Abs 5 der Richtlinie 2003/48/EG.“⁶²

Es ergeben sich daher folgende Alternativen zum Quellensteuerabzug:

- Optierung als OGAW,
- Verzicht auf das Bankgeheimnis.

Optierung als OGAW

Unter OGAW versteht man einen Organismus für gemeinsame Anlagen in Wertpapieren, der gem der RL 85/611/EWG⁶³ zugelassen ist. Zu betonen ist, dass der RL 2003/48/EG grundsätzlich nur natürliche Personen unterliegen. OGAW sind zusätzlich zu den juristischen Personen explizit genannt und fallen daher nicht in den Anwendungsbereich der Richtlinie.⁶⁴

Verzicht auf das Bankgeheimnis

Beim Verzicht auf das Bankgeheimnis wird ein vereinfachter Informationsaustausch durchgeführt. Dieser wird in § 2 Abs 2 Eu-QuStG umschrieben: (...) „Der Wirtschaftsbeteiligte (hat) den Namen und die Anschrift der Einrichtung sowie den Gesamtbetrag der zu Gunsten dieser Einrichtung gezahlten oder eingezogenen Zinsen der zuständigen Behörde mitzuteilen, welche diese Informationen an die zuständige Behörde des Mitgliedstaates weiterleitet, in dem die betreffende Einrichtung niedergelassen ist

⁶⁰ Vgl 19. Erwägungsgrund der RL 2003/48/EG.

⁶¹ Vgl besonders 350 der Beilagen XXII. GP – Regierungsvorlage – Materialien, Besonderer Teil, Zu Artikel II, zu § 4.

⁶² 350 der Beilagen XXII. GP – Regierungsvorlage – Materialien, Besonderer Teil, Zu Artikel II, zu § 4 Abs 3.

⁶³ Richtlinie 85/611/EWG des Rates vom 20. Dezember 1985 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl L 375 vom 31.12.1985, S 3–18).

⁶⁴ Zu Problemen der Anwendung der Zinssteuer-RL bei Zwischenschaltung von juristischen Personen oder Rechtsvereinbarungen wie bestimmten Stiftungen oder Trusts: *Aigner*, Problembereiche bei der Behandlung von Trusts und Stiftungen im Anwendungsbereich der Sparzinsenrichtlinie, ZfS 2009, 59 (59 ff); kritisch zum Änderungsvorschlag der EK vom 13.11.2008: *Knörzer*, Reform der EU-Zinsenbesteuerung: Auswirkungen auf Stiftungen, SWI 2009, 274 (278 f).

(vereinfachter Informationsaustausch).“⁶⁵ Dies ermöglicht eine Besteuerung der Zinseinkünfte im Staat, in dem die Einrichtung niedergelassen ist. Die Materialien zur Regierungsvorlage erklären die damit im Zusammenhang stehende Regelung des § 4 Abs 2 Eu-QuStG anhand eines Beispiels:

*Eine österreichische Bank zahlt Zinsen an eine Einrichtung gem § 4 Abs 2, die in einem anderen Mitgliedstaat niedergelassen ist. Die Einrichtung hat nicht optiert, jedoch ausdrücklich auf die Anwendung des Bankgeheimnisses verzichtet. Die österreichische Bank gibt der zuständigen österreichischen Behörde Namen und Anschrift der Einrichtung und den Gesamtbetrag der an die Einrichtung gezahlten oder [zu] deren Gunsten eingezogenen Zinsen bekannt. Die zuständige österreichische Behörde leitet diese Information an die zuständige Behörde des Mitgliedstaates weiter, in dem die Einrichtung niedergelassen ist (vereinfachter Informationsaustausch). Die Einrichtung wird im Zeitpunkt der Vereinnahmung der Zinsen zur Zahlstelle (Zahlstelle durch Vereinnahmung) und hat daher ihrerseits die Verpflichtungen zu erfüllen, die sich aus der Umsetzung der Richtlinie ergeben. Dh die Einrichtung hat im Zeitpunkt der Vereinnahmung Informationen zu liefern oder, falls die Einrichtung in Belgien oder Luxemburg niedergelassen ist, eine Quellensteuer einzubehalten, soweit wirtschaftliche Eigentümer aus einem anderen Mitgliedstaat beteiligt sind.*⁶⁶

(3) Strukturelle Unterschiede = Bankgeheimnis?!

Die Gründe für die Übergangsbestimmungen für Belgien, Luxemburg und Österreich sind daher vor allem im Bankgeheimnis zu sehen. Die in Art 8 der RL 2003/48/EG detailliert beschriebenen Auskunftspflichten „über sämtliche während eines Steuerjahrs erfolgten Zinszahlungen werden mindestens einmal jährlich automatisch erteilt, und zwar binnen sechs Monaten nach dem Ende des Steuerjahres des Mitgliedstaats, in dem die Zahlstelle niedergelassen ist.“⁶⁷ Die Auskünfte können nicht erteilt werden, soweit sie einer Geheimnispflicht unterliegen. Hierfür wurde die Pauschalabgeltung durch die Quellensteuer geschaffen. Der Grund für die Schaffung der Quellensteuer ist daher in den damals in Belgien, Luxemburg und Österreich stark ausgeprägten Bankgeheimnissen zu sehen, die zum Zeitpunkt des Inkrafttretens der RL 2003/48/EG einen automatischen Informationsaustausch nicht ermöglichten.⁶⁸

⁶⁵ § 2 Abs 2 letzter Satz EuQuStG.

⁶⁶ 350 der Beilagen XXII. GP – Regierungsvorlage – Materialien, Besonderer Teil, Zu Artikel II, zu § 4 Abs 2.

⁶⁷ Art 9 Abs 2 der RL 2003/48/EG.

⁶⁸ Vgl auch Gläser, EU-Zinsenbesteuerung – Vermeidung der Doppelbesteuerung, SWI 2005, 325.

2. Automatische Auskunftserteilung

a) Begriff

Im Kapitel II der RL 2003/48/EG ist die Auskunftserteilung geregelt, wobei Art 8 leg cit allgemein die von der Zahlstelle zu erteilenden Auskünfte aufzählt⁶⁹ und Art 9 im Besonderen auf die Automatische Auskunftserteilung eingeht⁷⁰.

(1) Art 8 der RL 2003/48/EG

Um eine rein deskriptive Arbeit zu vermeiden, werde ich nur kurz die Grundzüge dieser Regelung darlegen: Fällt die Zinszahlung in den Anwendungsbereich der Richtlinie (wirtschaftlicher Eigentümer der Zinsen ist nicht im gleichen Mitgliedstaat ansässig, wie die Zahlstelle), so hat die Zahlstelle der zuständigen Behörde mindestens folgende Auskünfte zu erteilen:

- Identität und Wohnsitz des gemäß Artikel 3 festgestellten wirtschaftlichen Eigentümers,
- Name und Anschrift der Zahlstelle,
- Kontonummer des wirtschaftlichen Eigentümers oder, in Ermangelung einer solchen, Kennzeichen der Forderung, aus der die Zinsen herrühren, und
- Auskünfte zur Zinszahlung gemäß Art 8 Abs 2 der RL 2003/48/EG.⁷¹

Art 8 Abs 2 der RL geht auf die sich aus den unterschiedlichen Definitionen der „Zinszahlung“ (vgl Art 6 der RL) ergebenden Unterschiede bei der Zinshöhe und damit des zu meldenden Betrages ein.

(2) Art 9 der RL 2003/48/EG

Art 9 der RL behandelt die Automatische Auskunftserteilung. Demnach sind die zuvor beschriebenen „Auskünfte nach Art 8 der zuständigen Behörde des Mitgliedstaats, in dem der wirtschaftliche Eigentümer ansässig ist“⁷², zu erteilen. Diese Auskünfte erteilt somit die

⁶⁹ Vgl Art 8 der RL 2003/48/EG: Von der Zahlstelle zu erteilende Auskünfte.

⁷⁰ Vgl Art 9 der RL 2003/48/EG: Automatische Auskunftserteilung.

⁷¹ Vgl Art 8 Abs 1 der RL 2003/48/EG.

⁷² Art 9 Abs 1 der RL 2003/48/EG.

zuständige Behörde des Mitgliedstaats, in dem sich die Zahlstelle befindet, der zuständigen Behörde des Mitgliedstaats, in dem der wirtschaftliche Eigentümer ansässig ist.

Art 9 Abs 2 der RL 2003/48/EG regelt die Häufigkeit der automatischen Auskünfte: „Die Auskünfte über sämtliche während eines Steuerjahrs erfolgten Zinszahlungen werden mindestens einmal jährlich automatisch erteilt, und zwar binnen sechs Monaten nach dem Ende des Steuerjahres des Mitgliedstaats, in dem die Zahlstelle niedergelassen ist.“⁷³

Art 9 Abs 3 leg cit bestimmt, dass subsidiär die Bestimmungen der RL 77/799/EWG⁷⁴ gelten, wengleich Art 8 der RL 77/799/EWG (Grenzen des Auskunftsaustausches) für jene Auskünfte nach Kapitel II der RL 2003/48/EG nicht zu beachten ist.

b) Ausnahmen von der automatischen Auskunftserteilung

Im 18. Erwägungsgrund der RL 2003/48/EG heißt es, dass zur Vermeidung von Ungleichbehandlungen Österreich, Belgien und Luxemburg nicht verpflichtet sein sollen, die automatische Auskunftserteilung anzuwenden, „bevor die Schweizerische Eidgenossenschaft, das Fürstentum Andorra, das Fürstentum Liechtenstein, das Fürstentum Monaco und die Republik San Marino die effektive Auskunftserteilung über Zinszahlungen auf Ersuchen sicherstellen“⁷⁵.

Österreich, Belgien und Luxemburg sollten ein Verfahren vorsehen, das es in anderen Mitgliedstaaten steuerlich ansässigen wirtschaftlichen Eigentümern ermöglicht, die Erhebung der Quellensteuer dadurch zu vermeiden, dass sie ihre Zahlstelle zur Meldung der Zinszahlungen ermächtigen oder dass sie eine von der zuständigen Behörde des Mitgliedstaates, in dem sie steuerlich ansässig sind, ausgestellte Bescheinigung vorlegen. Es besteht somit die Möglichkeit, den Quellensteuerabzug zu vermeiden, wenn auf das Bankgeheimnis verzichtet wird.

⁷³ Art 9 Abs 2 der RL 2003/48/EG.

⁷⁴ Richtlinie 77/799/EWG des Rates vom 19. Dezember 1977 über die gegenseitige Amtshilfe zwischen den zuständigen Behörden der Mitgliedstaaten im Bereich der direkten Steuern (ABl L 336 vom 27.12.1977, S 15-20).

⁷⁵ Erwägungsgrund 18 der RL 2003/48/EG.

c) Höhe der Quellensteuer

Art 11 der RL 2003/48/EG legt die Höhe der Quellensteuer während des Übergangszeitraumes⁷⁶ fest. Demnach soll in Belgien, Luxemburg und Österreich während der ersten drei Jahre der Übergangszeit eine Quellensteuer in Höhe von 15 %, in den darauf folgenden drei Jahren eine Quellensteuer in Höhe von 20 % und danach eine Quellensteuer in Höhe von 35 % erhoben werden.⁷⁷

Abs 2 leg cit beschreibt die Modalitäten, wie die Zahlstelle die Quellensteuer einbehalten soll. Hierbei wird nach den unterschiedlichen Zinszahlungen, welche in Art 6 der RL 2003/48/EG umschrieben werden, unterschieden und sodann die Bemessungsgrundlage der Quellensteuer dargelegt:⁷⁸

a) auf ein Konto gezahlte oder einem Konto gutgeschriebene Zinsen, die mit Forderungen jeglicher Art zusammenhängen, unabhängig davon, ob diese hypothekarisch gesichert sind oder nicht und ob sie ein Recht auf Beteiligung am Gewinn des Schuldners beinhalten oder nicht, insbesondere Erträge aus Staatspapieren, Anleihen und Schuldverschreibungen einschließlich der mit diesen Titeln verbundenen Prämien und Gewinne, wobei Zuschläge für verspätete Zahlungen nicht als Zinszahlung gelten⁷⁹: **auf den Betrag der gezahlten oder gutgeschriebenen Zinsen.**

b) bei Abtretung, Rückzahlung oder Einlösung von Forderungen im Sinne von Buchstabe a) aufgelaufene oder kapitalisierte Zinsen sowie Erträge, die bei Abtretung, Rückzahlung oder Einlösung von Anteilen an den nachstehend aufgeführten Organismen und Einrichtungen realisiert werden, wenn diese direkt oder indirekt über nachstehend aufgeführte andere Organismen für gemeinsame Anlagen oder Einrichtungen mehr als 40 % ihres Vermögens in den unter Buchstabe a) genannten Forderungen angelegt haben:

- i) nach der Richtlinie 85/611/EWG zugelassene OGAW,
- ii) Einrichtungen, die von der Wahlmöglichkeit des Art 4 Abs 3 der RL 2003/48/EG (Behandlung als OGAW) Gebrauch gemacht haben,
- iii) außerhalb des räumlichen Geltungsbereiches der RL 2003/48/EG niedergelassene OGAW.

⁷⁶ Vgl folgender Punkt II.D.2.d) Beginn und Ende des Übergangszeitraumes.

⁷⁷ Art 11 Abs 1 der RL 2003/48/EG.

⁷⁸ Vgl auch *Höllinger*, Ab 1. Juli wird's ernst: Die neue EU-Zinsrichtlinie, VWT 2005 H 3, 48.

⁷⁹ Vgl Art 6 Abs 1 Buchstabe a) der RL 2003/48/EG.

Die Mitgliedstaaten brauchen jedoch die soeben genannten Erträge nur insoweit in die Definition der Zinsen einzubeziehen, wie sie Erträgen entsprechen, die mittelbar oder unmittelbar aus Zinszahlungen im Sinne der Buchstaben a) und b) stammen⁸⁰: **entweder auf den Betrag der bezeichneten Zinsen oder Erträge oder im Wege einer vom Empfänger zu entrichtenden Abgabe gleicher Wirkung auf den vollen Erlös aus Abtretung, Rückzahlung oder Einlösung.**

c) direkte oder über eine Einrichtung im Sinne von Art 4 Abs 2 der RL 2003/48/EG laufende Zinserträge, die ausgeschüttet werden von

i) nach der Richtlinie 85/611/EWG zugelassenen OGAW,

ii) Einrichtungen, die von der Wahlmöglichkeit des Art 4 Abs 3 der RL 2003/48/EG Gebrauch gemacht haben,

iii) außerhalb des räumlichen Geltungsbereiches der RL 2003/48/EG niedergelassene OGAW⁸¹: **auf den Betrag der bezeichneten Erträge.**

d) Werden Zinsen im Sinne von Art 6 Abs 1 der RL 2003/48/EG an eine Zahlstelle kraft Vereinnahmung im Sinne von Art 4 Abs 2 der RL 2003/48/EG gezahlt, der die Wahlmöglichkeit, sich als OGAW behandeln zu lassen (vgl Art 4 Abs 3 der RL 2003/48/EG) nicht eingeräumt wurde, oder einem Konto einer solchen Einrichtung gutgeschrieben, so gelten sie als Zinszahlung durch diese Einrichtung⁸²: **auf den Betrag der Zinsen, die den einzelnen Mitgliedern der Zahlstelle kraft Vereinnahmung, die die Voraussetzungen des Art 1 Abs 1 und Art 2 Abs 1 der RL 2003/48/EG erfüllen, zuzurechnen sind.**

e) In Bezug auf die Art 6 Abs 1 lit b) und d) der RL können die Mitgliedstaaten von den in ihrem Gebiet niedergelassenen Zahlstellen verlangen, Zinsen für einen Zeitraum von höchstens einem Jahr auf Jahresbasis umzurechnen, und solcherart umgerechnete Zinsen auch dann als Zinszahlung behandeln, wenn in diesem Zeitraum keine Abtretung, keine Rückzahlung und keine Einlösung erfolgt ist: **auf den Betrag der auf Jahresbasis umgerechneten Zinsen.**

⁸⁰ Vgl Art 6 Abs 1 Buchstabe b) und d) der RL 2003/48/EG.

⁸¹ Vgl Art 6 Abs 1 Buchstabe c) der RL 2003/48/EG.

⁸² Vgl Art 6 Abs 4 der RL 2003/48/EG.

Um die genaue Definition der Höhe der Zinszahlung zu beachten, verweise ich ergänzend auf die Sonderbestimmungen in Art 6 Abs 3 und Art 6 Abs 6 bis 8 der RL 2003/48/EG. Dort werden abweichende Regelungen postuliert.

Der Zinsbegriff der RL knüpft an Art 11 Abs 3 des OECD-MA⁸³ an und beinhaltet einen Zinsbegriff iwS, der sich sowohl aus einer materiellen (Zinsbegriff ieS) als auch aus einer formellen Komponente zusammensetzt.⁸⁴

Die Erträge können neben der Quellensteuer zusätzlich durch den Mitgliedstaat des steuerlichen Wohnsitzes des wirtschaftlichen Eigentümers besteuert werden, sofern dies mit dem Vertrag vereinbar ist.⁸⁵

Da der Anwendungsbereich dieser Richtlinie auf die Besteuerung von Zinserträgen aus Forderungen beschränkt werden sollte, bleiben unter anderem Fragen im Zusammenhang mit der Besteuerung von Renten und Versicherungsleistungen unberührt.⁸⁶

d) Beginn und Ende des Übergangszeitraumes

Für Belgien, Luxemburg und Österreich wird ein Übergangszeitraum definiert. Während dieser Zeit müssen die Bestimmungen des Kapitels II der RL 2003/48/EG („Auskunftserteilung“) nicht angewendet werden. Sie haben jedoch selber die Möglichkeit, Auskünfte nach Kapitel II von anderen Mitgliedstaaten zu erhalten.

Dies gilt jedoch nur, wenn die genannten Mitgliedstaaten eines der folgenden Verfahren oder beide Verfahren vorsehen, um zu gewährleisten, dass der wirtschaftliche Eigentümer beantragen kann, dass die Quellensteuer nicht einbehalten wird.⁸⁷

- ein Verfahren, das es dem wirtschaftlichen Eigentümer ausdrücklich gestattet, die Zahlstelle zur Erteilung der Auskünfte nach Kapitel II zu ermächtigen; diese Ermächtigung gilt für sämtliche Zinszahlungen dieser Zahlstelle an den betreffenden wirtschaftlichen Eigentümer;

⁸³ Musterabkommen der OECD zur Vermeidung der Doppelbesteuerung auf dem Gebiet der Steuern vom Einkommen und Vermögen (Model Tax Convention on Income and on Capital: Condensed Version 2000) – vgl http://www.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2000_mtc_cond-2000-en (Stand: 18.08.2013).

⁸⁴ Gläser, Handbuch der EU-Quellensteuer, S 88.

⁸⁵ Art 11 Abs 4 der RL 2003/48/EG.

⁸⁶ Vgl Erwägungsgrund 13 der RL 2003/48/EG.

⁸⁷ Vgl im Folgenden Art 13 Abs 1 der RL 2003/48/EG.

in diesem Falle ist Artikel 9 der RL 2003/48/EG (Automatische Auskunftserteilung) anzuwenden;

- ein Verfahren, das gewährleistet, dass keine Quellensteuer einbehalten wird, wenn der wirtschaftliche Eigentümer seiner Zahlstelle eine von der zuständigen Behörde des Mitgliedstaats seines steuerlichen Wohnsitzes auf seinen Namen ausgestellte Bescheinigung nach Art 13 Abs 2 der RL 2003/48/EG vorlegt.

Beginn des Übergangszeitraumes:

Der Übergangszeitraum beginnt mit dem Zeitpunkt der Anwendung der RL 2003/48/EG. Nach Art 17 Abs 2 der RL 2003/48/EG wenden die Mitgliedstaaten diese Vorschriften ab dem 1. Januar 2005 an, sofern

- die Schweizerische Eidgenossenschaft, das Fürstentum Liechtenstein, die Republik San Marino, das Fürstentum Monaco und das Fürstentum Andorra ab dem gleichen Zeitpunkt gemäß den von ihnen nach einstimmigem Beschluss des Rates mit der Europäischen Gemeinschaft geschlossenen Abkommen Maßnahmen anwenden, die den in dieser Richtlinie vorgesehenen Maßnahmen gleichwertig sind;

- alle Abkommen oder sonstigen Regelungen bestehen, die vorsehen, dass alle relevanten abhängigen oder assoziierten Gebiete (Kanalinseln, Isle of Man und abhängige oder assoziierte Gebiete in der Karibik) ab dem gleichen Zeitpunkt die automatische Auskunftserteilung in der in Kapitel II dieser Richtlinie vorgesehenen Weise anwenden (oder während des Übergangszeitraums nach Artikel 10 eine Quellensteuer in Übereinstimmung mit den Vorschriften der Artikel 11 und 12 erheben).

Ob diese Bedingungen erfüllt sind, stellt der Rat der Europäischen Union mindestens sechs Monate vor dem 1. Januar 2005 einstimmig fest.⁸⁸ In der Richtlinie ist für den Fall, dass der Rat nicht feststellt, dass die Bedingungen erfüllt sind, normiert, dass er einstimmig auf Vorschlag der Kommission einen neuen Zeitpunkt für die Zwecke des Art 17 Abs 2 der RL 2003/48/EG festlegt.

⁸⁸ Art 17 Abs 3 der RL 2003/48/EG.

Der Rat der Europäischen Union hat mit Entscheidung vom 19. Juli 2004⁸⁹ festgestellt, dass die in Art 17 Abs 2 der RL 2003/48/EG genannte Bedingung mit **1. Juli 2005** erfüllt ist. Der Übergangszeitraum hat somit statt mit 1. Januar 2005 mit 1. Juli 2005 begonnen.

Ende des Übergangszeitraumes:

Art 10 Abs 2 der RL 2003/48/EG bestimmt, dass der Übergangszeitraum mit dem Ende des ersten abgeschlossenen Steuerjahrs endet, das auf den späteren der beiden nachstehenden Zeitpunkte folgt:

„— den Tag des Inkrafttretens eines nach einstimmigem Beschluss des Rates geschlossenen Abkommens zwischen der Europäischen Gemeinschaft und dem letzten der Staaten Schweizerische Eidgenossenschaft, Fürstentum Liechtenstein, Republik San Marino, Fürstentum Monaco, Fürstentum Andorra über die Auskunftserteilung auf Anfrage im Sinne des OECD-Musterabkommens zum Informationsaustausch in Steuersachen vom 18. April 2002 (im Folgenden „OECD-Musterabkommen“ genannt) hinsichtlich der in dieser Richtlinie definierten Zinszahlungen von im Hoheitsgebiet des jeweiligen Staates niedergelassenen Zahlstellen an wirtschaftliche Eigentümer, deren Wohnsitz sich im räumlichen Geltungsbereich der Richtlinie befindet, und der gleichzeitig erfolgenden Anwendung des in Artikel 11 Absatz 1 für den entsprechenden Zeitraum festgelegten Quellensteuersatzes auf derartige Zahlungen durch die vorstehend genannten Staaten;

— den Tag, an dem der Rat einstimmig zu der Auffassung gelangt, dass die Vereinigten Staaten von Amerika sich hinsichtlich der in dieser Richtlinie definierten Zinszahlungen von in ihrem Hoheitsgebiet niedergelassenen Zahlstellen an wirtschaftliche Eigentümer, deren Wohnsitz sich im räumlichen Geltungsbereich der Richtlinie befindet, zur Auskunftserteilung auf Anfrage im Sinne des OECD Musterabkommens verpflichtet haben.“⁹⁰

Sobald der Übergangszeitraum zu Ende ist, müssen Belgien, Luxemburg und Österreich die Bestimmungen des Kapitels II anwenden. Zum gleichen Zeitpunkt wird in diesen Ländern die

⁸⁹ Vgl 2004/587/EG Entscheidung des Rates vom 19. Juli 2004 zum Zeitpunkt der Anwendung der Richtlinie 2003/48/EG im Bereich der Besteuerung von Zinserträgen (ABl L 257 vom 04.08.2004, S 7–7).

⁹⁰ Art 10 Abs 2 der RL 2003/48/EG.

Erhebung der Quellensteuer und die Aufteilung der Einnahmen gemäß den Artikeln 11 und 12 der RL 2003/48/EG eingestellt.

Sollte sich Belgien, Luxemburg oder Österreich bereits während des Übergangszeitraums für die Anwendung der Bestimmungen des Kapitels II entscheiden, so stellen sie die Erhebung der Quellensteuer und die Aufteilung der Einnahmen gemäß den Artikeln 11 und 12 der RL 2003/48/EG ein.⁹¹

Weshalb die Anwendbarkeit der Richtlinie an die Umsetzung von Maßnahmen in Drittstaaten anknüpft, erklärt der 24. Erwägungsgrund der Richtlinie. Demnach könnte die Kapitalflucht hin zu den Vereinigten Staaten von Amerika, der Schweiz, Andorra, Liechtenstein, Monaco, San Marino und den relevanten abhängigen oder assoziierten Gebieten der Mitgliedstaaten die Erreichung der Ziele der Richtlinie gefährden. Es müssen daher Maßnahmen erlassen werden, die den Bestimmungen dieser Richtlinie gleichwertig sind oder sich mit diesen decken. Daher gilt die Richtlinie von dem Zeitpunkt an, zu dem alle diese Länder und Gebiete die entsprechenden Maßnahmen anwenden.⁹² Sofern die genannten Länder ihr Bankgeheimnis nicht abschaffen und den Informationsaustausch nicht durchführen, können auch die derzeit vom Anwendungsbereich des automatischen Informationsaustausches ausgenommenen EU-Mitgliedstaaten das Bankgeheimnis beibehalten und Quellensteuern erheben.⁹³

Die zweite Bedingung (Auskunftserteilung im Sinne des OECD-Musterabkommens durch die Vereinigten Staaten von Amerika) wird von der überwiegenden Mehrheit der EU-Staaten bereits als erfüllt angesehen.⁹⁴ In der Vergangenheit blockierten Österreich und Luxemburg den Abschluss von Steuerbetrugsabkommen mit den anderen Staaten und vertraten den Standpunkt, dass neben der formellen Umsetzung des Transparenzstandards im Bereich des Bankgeheimnisses, vor allem auch die Kriterien nach Art 26 Abs 5 des OECD-Musterabkommens erfüllt werden müssen, wonach Eigentümer- bzw Begünstigtenstruktur bei Gesellschaften, Trust und anderen ähnlichen Gebilden offen gelegt werden müssen.⁹⁵

⁹¹ Vgl Art 10 Abs 3 der RL 2003/48/EG.

⁹² Vgl 24. Erwägungsgrund der RL 2003/48/EG.

⁹³ *Höllinger*, Ab 1. Juli wird's ernst: Die neue EU-Zinsrichtlinie, VWT 2005 H 3, 48.

⁹⁴ *Lafite/Vondrak/Gruber*, Spiel mir das Lied vom Tod, Bankgeheimnis!, *ecolex* 2010, 82 (84).

⁹⁵ Vgl *Lafite/Vondrak/Gruber*, Spiel mir das Lied vom Tod, Bankgeheimnis!, *ecolex* 2010, 82 (84).

Die Europäische Kommission hat dem Rat am 15. September 2008 im ersten Bericht über die Anwendung der Zinssteuer-RL in den ersten drei Jahren ihrer Wirksamkeit⁹⁶ mehrere zu ergreifende Maßnahmen vorgeschlagen⁹⁷. Genannt seien etwa die Erweiterung des Zinsbegriffs der RL und gewisse Änderungen bei Investmentfonds zur Angleichung an die OGAW-Fonds.⁹⁸

Aktueller Stand in Belgien, Luxemburg und Österreich

Belgien hat die RL 2003/48/EG durch das „Loi transposant en droit belge la directive 2003/48/CE du 3 juin 2003 du Conseil de l'Union européenne en matière de fiscalité des revenus de l'épargne sous forme de paiements d'intérêts et modifiant le Code des impôts sur les revenus 1992 en matière de précompte mobilier“⁹⁹ in belgisches Recht transformiert. Mit Wirkung vom 1. Jänner 2010 hat Belgien statt der bis dahin praktizierten Quellensteuer den automatischen Informationsaustausch eingeführt,¹⁰⁰ sodass seit dem Meldezeitraum 2010 (01.01.2010 bis 31.12.2010) in Belgien keine Quellensteuer mehr erhoben wird.¹⁰¹

In Luxemburg wurde die RL 2003/48/EG durch das „Loi du 21 juin 2005 transposant en droit luxembourgeois la directive 2003/48/CE du 3 juin 2003 du Conseil de l'Union européenne en matière de fiscalité des revenus de l'épargne sous forme de paiement d'intérêts“¹⁰² und weiterer damit in Verbindung stehender Gesetze¹⁰³ umgesetzt. Zunächst wehrten sich

⁹⁶ Europäische Kommission, Bericht der Kommission gemäß Artikel 18 der RL 2003/48/EG des Rates im Bereich der Besteuerung von Zinserträgen vom 15.09.2008, KOM (2008) 552 endgültig, Ratsdokument 13124/08 FISC 117.

⁹⁷ Vgl. Aigner, Kommission veröffentlicht Bericht zur Überprüfung der Sparzinsenrichtlinie, SWI 2008, 505 (505 ff).

⁹⁸ Aigner, Europäische Kommission schlägt Änderungen der Sparzinsenrichtlinie zur Verhinderung der Steuerflucht vor, SWI 2008, 571 (573 ff); weitere vorgeschlagene Änderungen vgl. Aigner, Europäische Kommission schlägt Änderungen der Sparzinsenrichtlinie zur Verhinderung der Steuerflucht vor, SWI 2008, 571 (572 ff).

⁹⁹ Vgl. Moniteur Belge, Datum der Veröffentlichung: 27.05.2004, Seite: 41328-41334 – <http://www.ejustice.just.fgov.be/cgi/summary.pl> (Stand: 18.08.2013); Die Suche hat in französischer oder belgischer Sprache zu erfolgen – die deutsche Anzeige funktioniert nicht einwandfrei.

¹⁰⁰ Vgl. Moniteur Belge, Datum der Veröffentlichung: 01.10.2009, Seite: 65609-65615 (27.09.2009: Arrêté royal d'exécution de l'article 338bis, § 2, du Code des impôts sur les revenus 1992) sowie Moniteur Belge, Datum der Veröffentlichung: 01.10.2009, Seite 65615-65616 (27.09.2009: Arrêté royal relatif à l'entrée en vigueur de l'article 338bis, § 2, alinéas 1er à 3 du Code des impôts sur les revenus 1992) – <http://www.ejustice.just.fgov.be/cgi/summary.pl> (Stand: 18.08.2013).

¹⁰¹ Vgl. http://www.bzst.de/DE/Steuern_International/EU_Zinsrichtlinie/EU_Zinsrichtlinie_node.html (Stand: 18.08.2013); eine Länderübersicht inkl. der von Deutschland abgeschlossenen Abkommen in diesem Bereich vgl. http://www.bzst.de/DE/Steuern_International/EU_Zinsrichtlinie/Merkblaetter/Laenderaufstellung.html?nn=23300 (Stand: 18.08.2013).

¹⁰² Vgl. Mémorial Luxembourgeois A, Nummer: 86, Datum der Veröffentlichung: 22.06.2005, Seite: 01540-01546 – <http://www.legilux.public.lu> (Stand: 18.08.2013).

¹⁰³ Mémorial Luxembourgeois A, Nummer: 86, Datum der Veröffentlichung: 22.06.2005, Seite: 01547-01635 – <http://www.legilux.public.lu> (Stand: 18.08.2013).

Österreich und Luxemburg gemeinsam gegen den automatischen Informationsaustausch¹⁰⁴. Nach langem Ringen konnte nun ein politischer Konsens dahingehend gefunden werden, dass eine Veränderung notwendig ist. Noch vor Ende des Jahres 2013 soll die Zinssteuerrichtlinie geändert werden.¹⁰⁵ Auf internationaler Ebene soll bis 2014 ein globaler Standard für den automatischen Informationsaustausch definiert werden.¹⁰⁶

Nur erwähnen möchte ich an dieser Stelle das US-Gesetz „Foreign Account Tax Compliance Act“ (FATCA), womit „die USA ab 2013 alle Finanzinstitute der Welt zur Beschaffung von Informationen über Konten amerikanischer Bürger im Ausland verpflichten“¹⁰⁷ wollen. Durch zwischenstaatliche Verträge oder auch direkt mit den einzelnen Finanzinstituten aufgrund eines staatlichen Rahmenvertrages soll die Umsetzung erfolgen.¹⁰⁸

In Österreich hat sich das einst starke Auftreten gegen den automatischen Informationsaustausch¹⁰⁹ beruhigt.

Meine anfänglichen Bedenken, wie lange sich Österreich und Luxemburg noch gegen den Druck der anderen EU-Mitgliedstaaten wehren können, sind nun beinahe geklärt. Als Argumente für die Beibehaltung der Quellensteuer wurden von Österreich und Luxemburg immer die Bewahrung des Finanzplatzes, die entstehende unüberschaubare Zahl an Datenmengen und vor allem die Beibehaltung des jeweiligen nationalen Bankgeheimnisses angeführt.

Unzweifelhaft führt der jährliche (automatische) Informationsaustausch zu einer Fülle von personenbezogenen Daten, die jeweils an die Finanzbehörden des Wohnsitzstaates des Anlegers übermittelt werden müssen. Eine Verknüpfung dieser Daten sollte jedoch durch

¹⁰⁴ Zur damaligen politischen Blockadehaltung Österreichs und Luxemburgs: http://diepresse.com/home/wirtschaft/international/758532/Bankgeheimnis_Oesterreich-veraergert-EUKommission (Stand: 18.08.2013).

¹⁰⁵ http://diepresse.com/home/wirtschaft/eurokrise/1406161/Datenaustausch_Luxemburg-bremst-Oesterreich-stimmt-zu (Stand: 18.08.2013).

¹⁰⁶ <http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/global-forum-soll-automatischen-informationsaustausch-kontrollieren-1.18120173> (Stand: 18.08.2013).

¹⁰⁷ http://www.sif.admin.ch/00754/index.html?lang=de&download=NHZLpZeg7t,lnp6I0NTU04212Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXt8e2ym162epYbg2c_JjKbNoKSn6A-- – Seite 16 (Stand: 18.08.2013).

¹⁰⁸ Vgl aaO des schweizerischen Staatssekretariats für internationale Finanzfragen (SIF) – Seite 16 (Stand: 18.08.2013).

¹⁰⁹ Vgl Bericht zur Haltung der Bundesministerin für Finanzen Dr. Maria Fekter im Wirtschaftsblatt und DerStandard: <http://www.wirtschaftsblatt.at/home/oesterreich/wirtschaftspolitik/es-ging-nur-darum-unser-bankgeheimnis-auszuhebeln-518521/index.do> sowie <http://derstandard.at/1336696953222/EU-Steuerkommissar-Semeta-frustriert-wegen-Oesterreich> (Stand: 18.08.2013).

spezielle Programme möglich sein, zumal in 25 Mitgliedstaaten der EU dieses Verfahren bereits besteht. Die für mich bedeutsame Frage ist, worin der gravierende Unterschied zwischen Einkünften aus erbrachter Arbeit und Zinseinkünften aus Vermögen besteht.

Einerseits besteht nämlich die Pflicht zur Meldung des Einkommens aus erbrachter Arbeit und andererseits war eine Bewahrung des Bankgeheimnisses für Zinseinkünfte vorgesehen. Ich persönlich spreche mich daher für die Einführung des automatischen Informationsaustausches aus, womit eine weitere Aufweichung des österr Bankgeheimnisses verbunden ist.

Das lange diskutierte Abkommen zwischen der Republik Österreich und der Schweizerischen Eidgenossenschaft über die Zusammenarbeit in den Bereichen Steuern und Finanzmarkt¹¹⁰ wurde am 28.12.2012 kundgemacht. Dadurch soll in der Schweiz veranlagtes Vermögen und damit im Zusammenhang stehende Kapitaleinkünfte österreichischer Steuerpflichtiger durch eine Quellensteuer besteuert werden¹¹¹. Die Offenlegung der Identität der Personen soll jedoch verhindert werden. Darin äußert sich der politische Wille, den automatischen Informationsaustausch zu verhindern und andere mit dem Bankgeheimnis in Einklang stehende Wege zu beschreiten.

¹¹⁰ BGBl III 192/2012: Abkommen zwischen der Republik Österreich und der Schweizerischen Eidgenossenschaft über die Zusammenarbeit in den Bereichen Steuern und Finanzmarkt samt Schlussakte einschließlich der dieser beigefügten Erklärungen.

¹¹¹ Vgl V.D.2 Exkurs: Abkommen zwischen Österreich und Schweiz.

III. Akteure im Zusammenhang mit Datenaustausch

A. BMF

Das Bundesministerium für Finanzen (BMF) hat vor allem folgende zentralen Aufgaben: Budget- und Steuerpolitik sowie Fragen der Wirtschafts- und Strukturpolitik, des Zollwesens und der Informations- und Kommunikationstechnologie.¹¹²

Die Arbeit des Bundesministeriums für Finanzen ist auf sechs Sektionen aufgeteilt:

- Sektion I Präsidialsektion
- Sektion II Budget
- Sektion III Wirtschaftspolitik und Finanzmärkte
- Sektion IV Zölle und internationale sowie organisatorische Steuerangelegenheiten
- Sektion V IT, Kommunikation und Öffentlichkeitsarbeit
- Sektion VI Steuerpolitik und Materielles Steuerrecht

Hervorzuheben sind die Tätigkeiten der dritten und fünften Sektion. So setzt sich die Sektion „Wirtschaftspolitik und Finanzmärkte“ auch die Ziele, österreichische Interessen der Wirtschafts- und Finanzmarktpolitik bestmöglich in die internationale Diskussion einzubringen und optimale Rahmenbedingungen für den österreichischen Finanz- und Kapitalmarkt zu schaffen.¹¹³ Neben der Einbringung österreichischer Interessen in die internationale Debatte, „insbesondere in den Bereichen Banken-, Kapitalmarkt- und Versicherungsrecht“¹¹⁴, stellt die Wahrung der EU-Rechtskonformität des nationalen Rechtsbestandes im Bereich des Banken- und Kapitalmarktrechtes eine unter vielen anderen Tätigkeiten der Sektion dar.

Die fünfte Sektion, „IT, Kommunikation und Öffentlichkeitsarbeit“, soll ua Verwaltungsprozesse vereinfachen und Kosten senken.¹¹⁵ Hierbei kümmert sich diese Sektion

¹¹² Vgl <http://www.bmf.gv.at> (Stand: 18.08.2013).

¹¹³ https://www.bmf.gv.at/ministerium/aufgaben-organisation/zentraleitung.html#Sektion_III_Wirtschaftspolitik_und_Finanzm_rkte (Stand: 18.08.2013).

¹¹⁴ https://www.bmf.gv.at/ministerium/aufgaben-organisation/zentraleitung.html#Sektion_III_Wirtschaftspolitik_und_Finanzm_rkte (Stand: 18.08.2013).

¹¹⁵ https://www.bmf.gv.at/ministerium/aufgaben-organisation/zentraleitung.html#Sektion_V_IT_Kommunikation_und_ffentlichkeitsarbeit (Stand: 18.08.2013).

hauptsächlich um IT-Verfahren und IT-Unterstützung des Finanzministeriums selbst, sowie der gesamten Bundesverwaltung. Es sollen etwa Synergien durch ressortübergreifende IT-Verfahren entstehen.¹¹⁶

¹¹⁶ Vgl. https://www.bmf.gv.at/ministerium/aufgaben-organisation/zentraleitung.html#Sektion_V_IT_Kommunikation_und_oeffentlichkeitsarbeit (Stand: 18.08.2013).

B. FMA

Die 2002 gegründete österreichische Finanzmarktaufsicht (FMA) vereint die integrierte Aufsicht über alle wesentlichen Anbieter und Funktionen des Finanzmarktes. Die FMA beaufsichtigt Banken, Versicherer, Pensionskassen, Betriebliche Vorsorgekassen, Wertpapierfirmen und Wertpapierdienstleistungsunternehmen, Investmentfonds, Finanzkonglomerate sowie Börseunternehmen¹¹⁷. Sie hat folgende Aufgaben:

- *Die **Solvenzaufsicht** hat zum Ziel, dass die Banken, Versicherer und Finanzdienstleister jederzeit zahlungsfähig sind und ihren vertraglich eingegangenen Verpflichtungen nachkommen können. Da es das Wesen einer Marktwirtschaft ist, dass nicht mehr wettbewerbsfähige Institute ausscheiden, kann die Aufsicht jedoch nicht garantieren, dass nicht einzelne Institute sehr wohl insolvent werden und zu liquidieren sind. In diesen Fällen ist es das Ziel der Aufsicht, dafür Sorge zu tragen, dass das Ausscheiden ohne Erschütterung der Stabilität des Finanzmarktes und des Vertrauens in den Finanzmarkt erfolgt.*¹¹⁸
- *Die **Markt- und Verhaltensaufsicht** soll faire und transparente Verhältnisse auf den Märkten gewährleisten und darüber wachen, dass einerseits Mindeststandards in der Unternehmensführung andererseits in der Beratung und Information der Kunden eingehalten werden.*¹¹⁹
- *Besondere Bedeutung kommt auch den gesetzlichen Aufträgen zu, gegen unerlaubte Banken-, Versicherungs- und Finanzdienstleistungsgeschäfte vorzugehen sowie durch präventive Maßnahmen Geldwäsche und Terrorismusfinanzierung zu bekämpfen.*¹²⁰

Neben der Aufsicht durch die Finanzmarktaufsicht, die die einzelnen Finanzinstitute und Akteure überwacht und kontrolliert (Mikro-Aufsicht), sind auch die Oesterreichische Nationalbank (OeNB)¹²¹ und das Bundesministerium für Finanzen (BMF)¹²² zu erwähnen.¹²³ Das BMF entwickelt die rechtlichen Rahmenbedingungen, die dann vom österreichischen Parlament beschlossen werden (Rechtsetzung). Die OeNB „wacht über die Stabilität des

¹¹⁷ Vgl <http://www.fma.gv.at/de/ueber-die-fma/fma-auf-einen-blick.html> (Stand: 18.08.2013).

¹¹⁸ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/aufgaben-der-fma.html> (Stand: 18.08.2013).

¹¹⁹ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/aufgaben-der-fma.html> (Stand: 18.08.2013).

¹²⁰ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/aufgaben-der-fma.html> (Stand: 18.08.2013).

¹²¹ Vgl III.C OeNB.

¹²² Vgl III.A BMF.

¹²³ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/zusammenarbeit-mit-der-oenb.html> (Stand: 18.08.2013).

Finanzmarktes als Ganzes (Makro-Aufsicht), ist für die Aufsicht über Zahlungssysteme zuständig sowie in die Bankenaufsicht eingebunden¹²⁴, wobei seit 1. Jänner 2008 eine neue Form der Zusammenarbeit zwischen FMA und OeNB besteht¹²⁵, da auf die OeNB zusätzliche operative Aufsichtskompetenzen übertragen wurden^{126 127}.

	Meldewesen	Analyse	Prüfung	Behörde	Internationale Zusammenarbeit
ALT	FMA/OeNB	FMA/OeNB	OeNB	FMA	FMA/OeNB
NEU	OeNB	OeNB	OeNB	FMA	FMA

Aufsicht durch die FMA:

Die Aufsicht durch die FMA lässt sich – wie bereits beschrieben – in die „Solvenzaufsicht“ und die „Markt- und Verhaltensaufsicht“ unterteilen. Rechtliche Grundlagen sind etwa im Finanzmarktaufsichtsbehördengesetz¹²⁸, Nationalbankgesetz¹²⁹, Bankwesengesetz¹³⁰, Versicherungsaufsichtsgesetz¹³¹, Börsegesetz¹³² oder Kapitalmarktgesetz¹³³ geregelt.

Kernbereiche der Aufsicht über den österr Finanzmarkt sind die Bankenaufsicht, die Versicherungs- und Pensionskassenaufsicht sowie die Wertpapieraufsicht.¹³⁴

¹²⁴ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/zusammenarbeit-mit-der-oenb.html> (Stand: 18.08.2013).

¹²⁵ Zu den erfolgten Änderungen vgl. *Grabovickic/Dugonjic/Zinnöcker*, Bankenaufsicht in Österreich – Berichte und Analysen, ÖBA 2009, 425 (426), die eine positive Bewertung ziehen: *Grabovickic/Dugonjic/Zinnöcker*, Bankenaufsicht in Österreich – Berichte und Analysen, ÖBA 2009, 425 (430 f).

¹²⁶ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/zusammenarbeit-mit-der-oenb.html> (Stand: 18.08.2013).

¹²⁷ Grafik vgl: <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/zusammenarbeit-mit-der-oenb.html> (Stand: 18.08.2013).

¹²⁸ BGBl I Nr 97/2001, zuletzt geändert durch BGBl I Nr 160/2013: Bundesgesetz über die Errichtung und Organisation der Finanzmarktaufsichtsbehörde (Finanzmarktaufsichtsbehördengesetz - FMABG).

¹²⁹ BGBl Nr 50/1984 (WV), zuletzt geändert durch BGBl I Nr 64/2013: Bundesgesetz über die Oesterreichische Nationalbank (Nationalbankgesetz 1984 - NBG).

¹³⁰ BGBl Nr 532/1993, zuletzt geändert durch BGBl I Nr 135/2013: Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG).

¹³¹ BGBl Nr 569/1978, zuletzt geändert durch BGBl I Nr 83/2013: Bundesgesetz vom 18. Oktober 1978 über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz - VAG).

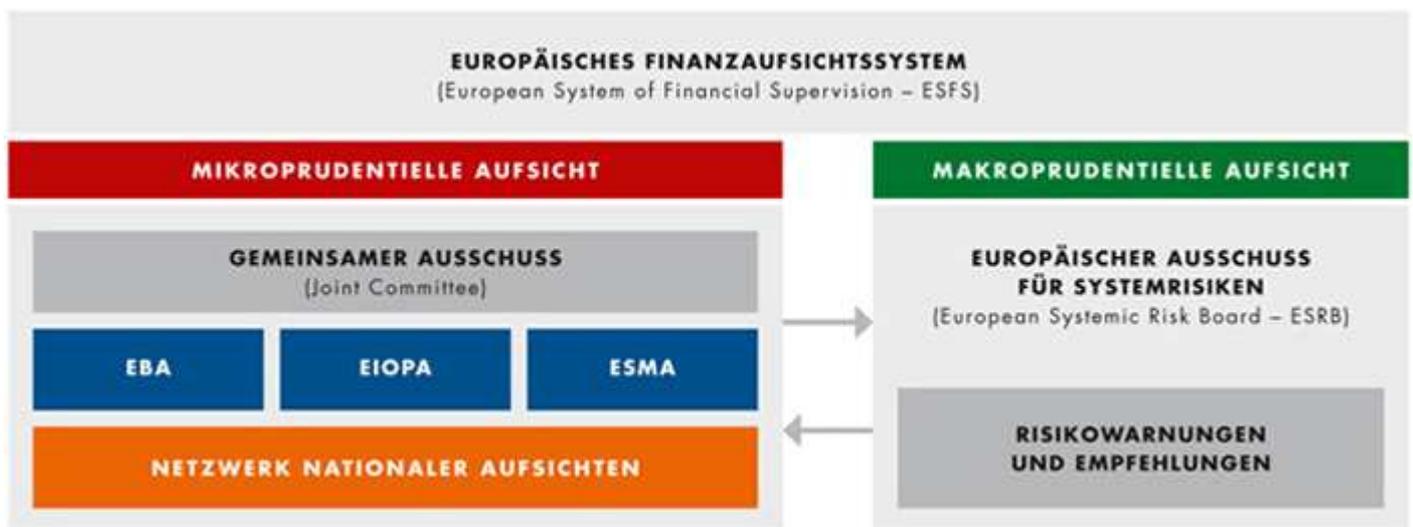
¹³² BGBl Nr 555/1989, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz vom 8. November 1989 über die Wertpapier- und allgemeinen Warenbörsen und über die Abänderung des Börsensensale-Gesetzes 1949 und der Börsegesetz-Novelle 1903 (Börsegesetz 1989 - BörseG).

¹³³ BGBl Nr 625/1991, zuletzt geändert durch BGBl I Nr 135/2013: Bundesgesetz über das öffentliche Anbieten von Wertpapieren und anderen Kapitalveranlagungen und über die Aufhebung des Wertpapier-Emissionsgesetzes (Kapitalmarktgesetz - KMG) sowie über die Abänderung des Aktiengesetzes 1965, des Genossenschaftsgesetzes, des Nationalbankgesetzes 1984, des Kreditwesengesetzes und des Versicherungsaufsichtsgesetzes.

¹³⁴ <http://www.fma.gv.at/de/ueber-die-fma/kompetenzen/aufgaben-der-fma.html> (Stand: 18.08.2013).

Europäisches und Internationales Umfeld:

„Mit 1. Jänner 2011 wurden die drei bestehenden Ausschüsse der Aufsichtsbehörden (CEBS, CEIOPS und CESR) durch Europäische Aufsichtsbehörden (EBA, EIOPA und ESMA) ersetzt, welche weitere Kompetenzen erhalten haben und deren Tätigkeiten weiterführen. Gleichzeitig wurde ein Europäischer Ausschuss für Systemrisiken (ESRB) errichtet.“¹³⁵¹³⁶



Bedeutende Mittel der internationalen aufsichtsbehördlichen Zusammenarbeit stellen die bilateralen oder auch multilateralen Memoranda of Understanding (MoU) sowie die Aufsichtskollegien (Supervisory Colleges) dar.¹³⁷

Im Bereich des Informationsaustausches sind etwa die Organisationen CEIOPS (Committee of European Insurance and Occupational Pensions Supervisors) und CESR (Committee of European Securities Regulators) bzw seit 1. Jänner 2011 EIOPA (European Insurance and Occupational Pensions Authority) und ESMA (European Securities and Markets Authority) sowie IOSCO (International Organization of Securities Commissions) zu erwähnen.

¹³⁵ <http://www.fma.gv.at/de/internationales/europaeische-aufsichtsarchitektur.html> (Stand: 18.08.2013).

¹³⁶ Grafik vgl: <http://www.fma.gv.at/de/internationales/europaeische-aufsichtsarchitektur.html> (Stand: 18.08.2013).

¹³⁷ Vgl <http://www.fma.gv.at/de/internationales/internationale-zusammenarbeit.html> (Stand: 18.08.2013).

C. OeNB

Durch den Eintritt Österreichs in die dritte Stufe der Wirtschafts- und Währungsunion haben sich die Rahmenbedingungen für die Oesterreichische Nationalbank (OeNB) grundlegend verändert.¹³⁸ „Mit der Einführung des Euro und der damit verbundenen geldpolitischen Architektur sind die Rollen der beteiligten europäischen Zentralbanken neu definiert worden.“¹³⁹

Folgende wesentlichen Aufgabengebiete umfasst die Tätigkeit der OeNB:¹⁴⁰

- geldpolitischer Entscheidungsprozess,
- Umsetzung der Geldpolitik,
- Kommunikation der Geldpolitik und
- Sicherung der Stabilität der Finanzmärkte.

Sicherheit, Stabilität und Vertrauen bestimmen weiterhin als Leitwerte die Ausübung dieser Aufgaben.¹⁴¹

Mit 1. Jänner 1999 wurde die OeNB Teil des Europäischen Systems der Zentralbanken (ESZB). Wesentliche rechtliche Bestimmungen für die OeNB als Zentralbank der Republik Österreich finden sich im „Vertrag über die Arbeitsweise der Europäischen Union“¹⁴², im Protokoll über die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank¹⁴³ und vor allem im Nationalbankgesetz 1984 (NBG)¹⁴⁴.¹⁴⁵

Die OeNB ist eine Aktiengesellschaft¹⁴⁶, dessen Grundkapital von 12 Millionen Euro zu 100% im Eigentum des Bundes steht¹⁴⁷, wobei sie in ihrer Funktion als nationale Zentralbank in völliger Unabhängigkeit zu agieren hat.

¹³⁸ <http://www.oenb.at> – Die OeNB – Aufgaben der OeNB; im ersten Absatz (Stand: 18.08.2013).

¹³⁹ <http://www.oenb.at> – Die OeNB – Aufgaben der OeNB; im ersten Absatz (Stand: 18.08.2013).

¹⁴⁰ Vgl <http://www.oenb.at> – Die OeNB – Aufgaben der OeNB; im vierten Absatz (Stand: 18.08.2013).

¹⁴¹ Vgl für Details: <http://www.oenb.at> – Die OeNB – Aufgaben der OeNB und Unterseiten (Stand: 18.08.2013).

¹⁴² Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union (ABl C 83 vom 30.03.2010, 47 ff), vgl vor allem Artt 127 ff und Artt 282 ff.

¹⁴³ Protokoll (Nr 4) über die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank (ABl C 83/230 ff vom 30.03.2010).

¹⁴⁴ BGBl Nr 50/1984 (WV), zuletzt geändert durch BGBl I Nr 50/2011: Bundesgesetz über die Oesterreichische Nationalbank (Nationalbankgesetz 1984 - NBG).

¹⁴⁵ Vgl <http://www.oenb.at> – Die OeNB – Rechtliche Grundlagen mit zahlreichen Verweisen (Stand: 18.08.2013).

¹⁴⁶ <http://www.oenb.at> – Die OeNB – Rechtliche Grundlagen; im zweiten Absatz (Stand: 18.08.2013).

¹⁴⁷ Vgl ebenda.

D. Kreditinstitute und andere Finanzinstitute

Von der österreichischen FMA werden folgende Unternehmen beaufsichtigt¹⁴⁸:

- 808 Kreditinstitute - davon 10 Betriebliche Vorsorgekassen
- 101 Versicherungsunternehmen
- 17 Pensionskassen mit 142 VRG, davon 8 überbetriebliche
- 88 Wertpapierfirmen und 79 Wertpapierdienstleistungsunternehmen
- 3 Finanzkonglomerate
- 2.230 inländische Investmentfonds von 24 Kapitalanlagegesellschaften
- 5.591 ausländische Investmentfonds
- 5 Immobilien-Kapitalanlagegesellschaften
- 373 Emittenten mit 9.041 gelisteten Wertpapieren

In dieser Arbeit werde ich vor allem auf die Kreditinstitute, Zahlungsinstitute und die E-Geld-Institute eingehen. Die in diesen Bereichen grundlegenden rechtlichen Rahmenbedingungen und die Differenzen bespreche ich an dieser Stelle kurz:

Kredit- und Finanzinstitute:

Ein Kreditinstitut ist, wer auf Grund der §§ 4 oder 103 Z 5 BWG oder besonderer bundesgesetzlicher Regelungen berechtigt ist, Bankgeschäfte zu betreiben.¹⁴⁹ Bankgeschäfte sind die in § 1 Abs 1 BWG aufgelisteten Tätigkeiten, soweit sie gewerblich durchgeführt werden.¹⁵⁰

In der Unternehmensdatenbank der FMA¹⁵¹ kann der Umfang der Konzession einer Bank oder anderer Unternehmensformen abgefragt werden. Die Konzession zum Betrieb von Bankgeschäften kann etwa mit Bedingungen und Auflagen versehen sein. Auch können Teile von einzelnen Bankgeschäften aus dem Konzessionsumfang ausgenommen sein.¹⁵²

¹⁴⁸ Stand: 16.5.2013; Quelle: <http://www.fma.gv.at/de/ueber-die-fma/fma-auf-einen-blick.html> (Stand: 18.08.2013).

¹⁴⁹ § 1 Abs 1 Satz 1 BWG.

¹⁵⁰ ZB Entgegennahme fremder Gelder zur Verwaltung oder als Einlage (Einlagengeschäft) [Z 1], die Durchführung des bargeldlosen Zahlungsverkehrs und des Abrechnungsverkehrs in laufender Rechnung für andere (Girogeschäft) [Z 2] oder der Abschluss von Geldkreditverträgen und die Gewährung von Gelddarlehen (Kreditgeschäft) [Z 3]; weitere Bankgeschäfte vgl § 1 Abs 1 Z 4 bis 22 BWG.

¹⁵¹ <http://www.fma.gv.at/de/unternehmen/suche-unternehmensdatenbank.html> (Stand: 18.08.2013).

¹⁵² Vgl <http://www.fma.gv.at/de/unternehmen/banken.html> (Stand: 18.08.2013).

Welche weiteren Geschäfte ein Kreditinstitut ausüben darf, ergibt sich abhängig von der Konzessionierung aus § 1 Abs 3 BWG.¹⁵³

Auch sind Kreditinstitute zur Durchführung aller sonstigen Tätigkeiten, die in unmittelbarem Zusammenhang mit der Banktätigkeit entsprechend dem jeweiligen Konzessionsumfang stehen oder Hilfstätigkeiten in Bezug auf diese darstellen, berechtigt, wozu auch die Erbringung von Dienstleistungen im Bereich der automatischen Datenverarbeitung zählt.¹⁵⁴

Im Unterschied dazu ist ein Finanzinstitut, wer kein Kreditinstitut im Sinne des Abs 1 leg cit ist und berechtigt ist, eine oder mehrere der in § 1 Abs 2 BWG genannten Tätigkeiten gewerbsmäßig durchzuführen, sofern er diese als Haupttätigkeit betreibt.¹⁵⁵ Außerdem ist § 2 Z 24 BWG zu beachten, der weitere vom Begriff der Finanzinstitute umfasste Rechtsgebilde umschreibt.¹⁵⁶

Der Betrieb der in § 1 Abs 1 BWG genannten Geschäfte bedarf der Konzession der FMA.¹⁵⁷ Ein Konzessionsantrag hat insbesondere die in § 4 Abs 3 und 4 BWG genannten Angaben und Unterlagen zu enthalten.

Für die Erteilung der Konzession müssen die in § 5 BWG genannten Voraussetzungen vorliegen. Insbesondere hat die FMA im Zuge des Konzessionsverfahrens die Zuverlässigkeit der Geschäftsleiter des Kreditinstitutes zu prüfen („fit & proper – Beurteilung“).¹⁵⁸

Gemäß § 6 Abs 1 BWG kann die FMA eine Konzession zurücknehmen, wenn der Geschäftsbetrieb, auf den sie sich bezieht, nicht innerhalb von zwölf Monaten nach Konzessionserteilung aufgenommen wurde oder dieser mehr als sechs Monate lang nicht ausgeübt worden ist.¹⁵⁹

¹⁵³ So sind Kreditinstitute etwa auch zur Durchführung der in Abs 1 Z 22 (Wechselstubengeschäft) und Abs 2 Z 1 bis 6 genannten Tätigkeiten berechtigt (vgl § 1 Abs 3 BWG).

¹⁵⁴ § 1 Abs 3 BWG.

¹⁵⁵ Vgl § 1 Abs 2 BWG: Der Abschluss von Leasingverträgen (Leasinggeschäft) [Z 1], die Beratung von Unternehmen über die Kapitalstruktur, die industrielle Strategie und in damit verbundenen Fragen sowie die Beratung und die Erbringung von Dienstleistungen auf dem Gebiet der Zusammenschlüsse und Übernahme von Unternehmen [Z 3], die Erteilung von Handelsauskünften [Z 5], die Erbringung von Schließfachverwaltungsdiensten [Z 6], die Erbringung von Zahlungsdiensten gemäß § 1 Abs 2 Zahlungsdienstegesetz – ZaDiG, BGBl I Nr 66/2009 [Z 7] oder die Ausgabe von E-Geld gemäß § 1 Abs 1 E-Geldgesetz 2010, BGBl I Nr 107/2010 [Z 8].

¹⁵⁶ § 2 Z 24 BWG.

¹⁵⁷ § 4 Abs 1 BWG.

¹⁵⁸ Vgl <http://www.fma.gv.at/de/unternehmen/banken/konzessionierung.html> (Stand: 18.08.2013).

¹⁵⁹ § 6 Abs 1 BWG.

Die FMA hat hingegen gemäß § 6 Abs 2 BWG eine Konzession zurücknehmen, wenn sie etwa durch unrichtige Angaben erschlichen wurde oder das Konkursverfahren über das Vermögen des Kreditinstituts eröffnet wurde.¹⁶⁰

Die Konzession erlischt nach § 7 Abs BWG ex lege durch Zeitablauf, bei Eintritt einer auflösenden Bedingung (§ 4 Abs 2 BWG), mit ihrer schriftlichen Zurücklegung¹⁶¹, mit der Eintragung der Verschmelzung oder Spaltung von Kreditinstituten in das Firmenbuch des übertragenden Kreditinstitutes oder der übertragenden Kreditinstitute sowie mit der Eintragung der Gesamtrechtsnachfolge auf Grund einer Einbringung gemäß § 92 BWG in das Firmenbuch hinsichtlich des doppelten oder mehrfachen Konzessionsbestandes bei einem Institut sowie mit der Eintragung der Europäischen Gesellschaft (SE) oder Europäischen Genossenschaft (SCE) in das Register des neuen Sitzstaates. Das Erlöschen der Konzession ist von der FMA durch Bescheid festzustellen.¹⁶²

Zahlungsinstitute:

„Zahlungsinstitute sind Unternehmen, die aufgrund einer Konzession der FMA oder aber einer Bewilligung einer Aufsichtsbehörde eines anderen EU-Mitgliedstaates zur gewerblichen Erbringung und Ausführung von Zahlungsdiensten im gesamten Gebiet der Europäischen Gemeinschaft berechtigt sind.“¹⁶³

Die konzessionspflichtigen Zahlungsdienste finden sich in § 1 Abs 2 ZaDiG¹⁶⁴.

Gemäß § 1 Abs 3 ZaDiG sind auch Kreditinstitute, E-Geld-Institute, die Österreichische Post AG hinsichtlich ihres Geldverkehrs, die Europäische Zentralbank, die OeNB und andere Nationalbanken des EWR, soweit sie nicht in ihrer Eigenschaft als Währungsbehörde handeln, Bund, Länder und die Gemeinden, soweit sie im Rahmen der Privatwirtschaftsverwaltung Zahlungsdienste erbringen, Zahlungsdienstleister. Insbesondere das Einlagengeschäft kann aber von den Zahlungsinstituten im Unterschied zu den Kreditinstituten nicht durchgeführt werden.

¹⁶⁰ Vgl § 6 Abs 2 Z 1 bis 5 BWG.

¹⁶¹ § 7 Abs 3 BWG ist hierbei zu beachten, der eine schriftliche Zurücklegung vorschreibt und dies nur für zulässig erachtet, sofern sämtliche Bankgeschäfte zuvor abgewickelt worden sind.

¹⁶² § 7 Abs 2 BWG.

¹⁶³ <http://www.fma.gv.at/de/unternehmen/zahlungsinstitute.html> (Stand: 18.08.2013).

¹⁶⁴ BGBl I Nr 66/2009, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG).

Das Zahlungsdienstegesetz ist erstmals mit 1.11.2009 in Kraft getreten.¹⁶⁵ Damit wurden die Erbringungen von Zahlungsdiensten detailliert geregelt und die Zahlungsinstitute eingeführt. Es setzt die europäische Richtlinie 2007/64/EG¹⁶⁶, die sogenannte Zahlungsdiensterichtlinie (Payment Services Directive - PSD) um. Die PSD schafft einen einheitlichen rechtlichen Rahmen für Zahlungsdienste und somit die nötige rechtliche Basis für einen einheitlichen Euro-Zahlungsverkehrsraum¹⁶⁷ (Single European Payment Area – SEPA¹⁶⁸).

Das ZaDiG schafft Verpflichtungen für alle Erbringer von Zahlungsdienstleistungen, vor allem für Kreditinstitute, Zahlungsinstitute und E-Geld-Institute. Die Erbringung von Zahlungsdiensten wie insbesondere Überweisungen, Kreditkartenzahlungen und Bezahlen mit dem Mobiltelefon war bisher nur in Grundzügen oder gar nicht geregelt.¹⁶⁹ Mehrere Bestimmungen schaffen nunmehr genaue Vorgaben. So muss etwa seit dem 1. Jänner 2012 der Betrag, der Gegenstand eines elektronischen Zahlungsvorganges ist, spätestens am Ende des dem Tag des Eingangszeitpunktes folgenden Geschäftstages gutgeschrieben werden.¹⁷⁰ Die Verbraucher- und Kundenrechte finden sich im dritten Hauptstück (Zahlungsdienste).¹⁷¹

Da die Zahlungsinstitute Dienstleistungen erbringen, die in Österreich bis 1.11.2009 ausschließlich Kreditinstituten vorbehalten waren, sind die aufsichtsbehördlichen Anforderungen jenen der Kreditinstitute nachempfunden. Details zur Konzessionierung von Zahlungsinstituten sind den §§ 5 bis 11 ZaDiG zu entnehmen.¹⁷²

E-Geld-Institute:

„E-Geld bezeichnet jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne von § 3 Z 5 ZaDiG

¹⁶⁵ Vgl § 79 Abs 1 ZaDiG.

¹⁶⁶ Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (ABl L 319 vom 05.12.2007, S 1–36).

¹⁶⁷ *Wagner/Eigner*, Aufsichtsrechtliche Aspekte der Zahlungsdiensterichtlinie, ÖBA 2008, 633 (634).

¹⁶⁸ Vgl V.C.2 SEPA – Single European Payment Area.

¹⁶⁹ Vgl <http://www.fma.gv.at/de/unternehmen/zahlungsinstitute.html> (Stand: 18.08.2013).

¹⁷⁰ § 42 Abs 1 ZaDiG.

¹⁷¹ §§ 26 bis 48 ZaDiG.

¹⁷² Vgl auch <http://www.fma.gv.at/de/unternehmen/zahlungsinstitute/konzessionierung.html> (Stand: 18.08.2013).

durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird.“ (§ 1 Abs 1 E-Geldgesetz¹⁷³)

Wann eine Konzession als E-Geld-Institut erteilt werden kann und weitere Bestimmungen zur Konzessionierung enthalten die §§ 3 bis 8 E-Geldgesetz. Ein E-Geld-Institut kann E-Geld gewerblich ausgeben und – je nach Umfang der Konzession – auch weitere Zahlungsdienste iSd § 1 Abs 2 ZaDiG erbringen oder auch Zahlungssysteme betreiben.¹⁷⁴

E-Geldinstitute sind daher im Unterschied zu den Zahlungsinstituten zusätzlich zu den Zahlungsdiensten gemäß ZaDiG auch zur Ausgabe von E-Geld berechtigt. Über noch weiter gehende Möglichkeiten (zB das Einlagengeschäft) verfügen – je nach Umfang der Konzession – die Kreditinstitute. Auch können E-Geld-Institute nur in eingeschränktem Umfang Kredite vergeben.¹⁷⁵

Ebenso wie bei den Zahlungsdiensten dürfen auch Kreditinstitute, die OeNB und andere in § 1 Abs 2 E-Geldgesetz genannte Unternehmen und Gebietskörperschaften E-Geld ausgeben.¹⁷⁶

Das E-Geldgesetz 2010 trat am 30.04.2011 in Kraft.¹⁷⁷ Es regelt unter welchen Bedingungen E-Geld an Kunden ausgegeben werden darf, sowie welches die Voraussetzungen zur Erlangung einer Konzession als E-Geld-Institut sind. Gemäß § 17 E-Geldgesetz hat der E-Geld-Emittent das E-Geld stets in der Höhe des Nennwertes des entgegengenommenen Geldbetrages auszugeben. Auch der Rücktausch, die Rücktauschbedingungen sowie dafür erlaubte Entgelte werden im E-Geldgesetz¹⁷⁸ geregelt.¹⁷⁹

Durch das E-Geldgesetz wird die RL 2009/110/EG (E-Geld-Richtlinie)¹⁸⁰ umgesetzt. Die bis zur RL 2009/110/EG geltende RL 2000/46/EG¹⁸¹ wurde vom Markt nicht so angenommen,

¹⁷³ BGBl I Nr 107/2010, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz über die Ausgabe von E-Geld und die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz 2010).

¹⁷⁴ Vgl § 3 E-Geldgesetz.

¹⁷⁵ Vgl <http://www.fma.gv.at/de/unternehmen/e-geld-institute.html> (Stand: 18.08.2013).

¹⁷⁶ § 1 Abs 2 E-Geldgesetz.

¹⁷⁷ § 41 E-Geldgesetz.

¹⁷⁸ § 18 und 19 E-Geldgesetz.

¹⁷⁹ Vgl auch <http://www.fma.gv.at/de/unternehmen/e-geld-institute.html> (Stand: 18.08.2013).

¹⁸⁰ Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl L 267 vom 10.10.2009, S 7–17).

wie es von vom europäischen Gesetzgeber gewünscht war. Vor allem enthielt sie eine unklare Definition des E-Geldes, eine unscharfe Abgrenzung zu anderen Zahlungsdiensten (zB Überweisung), sowie nur ein sehr eingeschränkt zulässiges Tätigkeitgebiet für E-Geld-Institute.¹⁸²

Eine wesentliche Neuerung ist, dass E-Geld-Institute nun auch Zahlungsdienste iSd § 1 Abs 2 ZaDiG¹⁸³ erbringen können.

Der genaue Konzessionsumfang von Kreditinstituten, Zahlungsinstituten, E-Geldinstituten und anderen von der FMA zu konzessionierenden Unternehmensformen kann auf der Webseite der FMA abgerufen werden. Darin finden sich etwa auch alle E-Geld-Institute aus anderen EU-Mitgliedstaaten, die in Österreich im Wege der Dienstleistungs- oder Niederlassungsfreiheit tätig sind.¹⁸⁴

¹⁸¹ Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (ABl L 275 vom 27.10.2000, S 39–43).

¹⁸² Vgl <http://www.fma.gv.at/de/unternehmen/e-geld-institute.html> (Stand: 18.08.2013).

¹⁸³ Dazu zählen etwa das Zahlungskartengeschäft (§ 1 Abs 2 Z 2 lit b ZaDiG) und das Überweisungsgeschäft (§ 1 Abs 2 Z 2 lit c ZaDiG).

¹⁸⁴ <http://www.fma.gv.at/de/unternehmen/e-geld-institute/konzessionierung.html> sowie die direkte Abfrage unter <http://www.fma.gv.at/de/unternehmen/suche-unternehmensdatenbank.html> (Stand: 18.08.2013).

E. Datenschutzkommission und Datenschutzrat

1. Allgemeines

Unbeschadet der Zuständigkeit des Bundeskanzlers¹⁸⁵ und der ordentlichen Gerichte¹⁸⁶ sind zur Wahrung des Datenschutzes nach den Bestimmungen des DSG die Datenschutzkommission (DSK) und der Datenschutzrat berufen.¹⁸⁷

Die Verfassungsbestimmung des § 35 Abs 2 DSG stellt sicher, dass die DSK ihre Befugnisse auch gegenüber den in Art 19 B-VG bezeichneten obersten Organen der Vollziehung ausüben kann¹⁸⁸.¹⁸⁹

2. Datenschutzkommission

a) Grundzüge der Datenschutzkommission

Mitglieder der Datenschutzkommission:

Die DSK besteht gemäß § 36 Abs 1 DSG aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden, wobei Wiederbestellungen zulässig sind¹⁹⁰. Für jedes Mitglied ist auch ein Ersatzmitglied zu bestellen.

Die Mitglieder müssen rechtskundig sein¹⁹¹, sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen¹⁹², dürfen nicht Mitglieder der Bundesregierung oder einer Landesregierung

¹⁸⁵ Vgl § 6 Abs 4, § 16 Abs 3, § 17 Abs 2 Z 6 und § 55 Z 1 und 2 DSG.

¹⁸⁶ Vgl §§ 32 bis 34 für die Zivilgerichtsbarkeit und § 51 für die Strafgerichtsbarkeit.

¹⁸⁷ § 35 Abs 1 DSG; vgl auch *Pollirer/Weiss/Knyrim*, DSG (2010) § 35.

¹⁸⁸ § 35 Abs 2 DSG und *Jahnel*, Handbuch Datenschutzrecht, 9/4 mit Verweis auf den Bundespräsidenten, die Bundesregierung, den Bundeskanzler, die (übrigen) Bundesminister, die Landesregierungen und die Landesräte als oberste Organe der Vollziehung.

¹⁸⁹ *Jahnel* weist auf die Aufhebung der Vorgängerbestimmung in § 14 DSG 1978 hin, die vor der Novelle BGBl 1994/632 mit Erk v 1.12.1993, G 139/93-141/93, VfSlg 13626/1993, als verfassungswidrig aufgehoben wurde, was durch die Erlassung des § 36 Abs 1 DSG 1978 als Verfassungsbestimmung saniert wurde. Das DSG 2000 übernahm diese Bestimmung in § 35 Abs 2 DSG. Nach stRsp des VfGH ist ein einem Bundesminister übergeordneter Instanzenzug ebenso wie die Betrauung eines Verwaltungsorgans mit der nachprüfenden Kontrolle der Rechtmäßigkeit seines Verhaltens verfassungsrechtlich unzulässig, weil ihm, wie sich aus Art 19 B-VG ergibt, die Stellung eines obersten Organs zukommt. Vgl dazu *Jahnel*, Zur Aufhebung von § 14 DSG durch den Verfassungsgerichtshof, EDVuR 1994, 94 und *Jahnel*, Datenschutzkommission verfassungsrechtlich abgesichert – Zur Datenschutzgesetznovelle 1994, wbl 1994, 401.

¹⁹⁰ § 36 Abs 1 DSG.

¹⁹¹ § 36 Abs 1 DSG.

¹⁹² § 36 Abs 2 DSG.

sowie Staatssekretäre sein und müssen zum Nationalrat wählbar sein¹⁹³. Sie üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus.¹⁹⁴

Der Bundeskanzler hat den Vorschlag der Bundesregierung für die Bestellung der Mitglieder der DSK vorzubereiten¹⁹⁵ und dabei auf folgende Vorschläge bedacht zu nehmen:

1. einen Dreivorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied,
2. einen Vorschlag der Länder für zwei Mitglieder¹⁹⁶,
3. einen Dreivorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied,
4. einen Dreivorschlag der Wirtschaftskammer Österreich für ein Mitglied.¹⁹⁷

Ein weiteres Mitglied ist aus dem Kreise der rechtskundigen Bundesbediensteten¹⁹⁸ vorzuschlagen.¹⁹⁹

Rechte der Mitglieder der Datenschutzkommission:

- Vergütungsanspruch

Für die Anreise zu den Sitzungen der DSK sowie für in Ausübung ihrer Funktion erforderliche sonstige Dienstreisen haben die Mitglieder und Ersatzmitglieder der DSK Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) durch den Bundeskanzler nach Maßgabe der für Bundesbedienstete geltenden Rechtsvorschriften. Weiters haben sie Anspruch auf eine der Zeit und dem Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.²⁰⁰

¹⁹³ § 36 Abs 5 DSG.

¹⁹⁴ § 36 Abs 3a DSG idF der DSG-Novelle 2010.

¹⁹⁵ Vgl § 36 Abs 2 DSG.

¹⁹⁶ Dies erfolgt in der Praxis durch einen Beschluss der Landeshauptleuterkonferenz (vgl *Pollirer/Weiss/Knyrim*, DSG (2010) § 36 Anm 4).

¹⁹⁷ Vgl § 36 Abs 2 DSG.

¹⁹⁸ Seit der DSG-Novelle 2010 wurde der Begriff „Bundesbeamten“ durch das Wort „Bundesbediensteten“ ersetzt, wodurch nunmehr klargestellt ist, dass sowohl Bundesbeamte als auch Vertragsbedienstete vorgeschlagen werden können (vgl *Pollirer/Weiss/Knyrim*, DSG (2010) § 36 Anm 5).

¹⁹⁹ § 36 Abs 3 DSG idF der DSG-Novelle 2010.

²⁰⁰ Vgl § 36 Abs 9 DSG und BGBl II 2006/145: VO der Bundesregierung, mit der die VO über die Vergütung für die Mitglieder der DSK geändert wird.

- Weisungsfreiheit

Die Mitglieder der DSK sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.²⁰¹ Die DSK ist als Kollegialbehörde mit richterlichem Einschlag gemäß Art 133 Z 4 B-VG entsprechend der verfassungsrechtlichen Ermächtigung des Art 20 Abs 2 B-VG in ihrer Funktion als entscheidendes, also bescheiderlassendes, Organ weisungsfrei gestellt.²⁰² Auf Grund dieser Bestimmung in § 37 Abs 1 DSG muss die DSK auch andere ihr zukommende Funktionen (insb § 30 Abs 6 und 6a – Empfehlungen zur Herstellung des rechtmäßigen Zustandes und andere Erhebung von Rechtsbehelfen) weisungsfrei besorgen.²⁰³ Hierzu ist das Verfahren der Europäischen Kommission gegen die Republik Österreich²⁰⁴ zu beachten, in dem das Kriterium der völligen Unabhängigkeit der DSK iSd Art 28 Abs 1 Satz 2 der RL 1995/46/EG von der Europäischen Kommission nicht als gegeben erachtet und vom EuGH bestätigt wurde.²⁰⁵

- Anhörungsrecht

Vor Erlassung von Verordnungen, die auf der Grundlage des DSG ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen, ist die DSK anzuhören.²⁰⁶ Nach Ansicht des VfGH ist der Funktionsbereich der „Art 133 Z 4-Behörden“ verfassungsrechtlich auf die individuelle Rechtskontrolle und die Streitentscheidung beschränkt, weshalb diese nicht zur Erlassung von VO ermächtigt werden dürfen.²⁰⁷ Die Nichtbeachtung des Anhörungsrechts der DSK zieht nach *Jahnel* und *Drobesh/Grosinger* Gesetzwidrigkeit der Verordnung nach sich.²⁰⁸ Dies wird aus einer Entscheidung des VfGH²⁰⁹ abgeleitet²¹⁰, in der die Unterlassung der Anhörung der Ortsbildpflegekommission einen wesentlichen Verfahrensmangel darstellte, der nach

²⁰¹ § 37 Abs 1 DSG.

²⁰² *Jahnel*, Handbuch Datenschutzrecht, 9/9 mit Verweis auf *Lehner/Lachmayr* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009), 116 f, die darüber hinaus aus § 1 Abs 5 DSG eine verfassungsrechtliche Absicherung der Weisungsfreistellung der DSK ableiten.

²⁰³ Vgl *Pollirer/Weiss/Knyrim*, DSG (2010) § 37 Anm 2.

²⁰⁴ Rechtssache C-614/10.

²⁰⁵ Vgl weiter unten.

²⁰⁶ § 38 Abs 3 DSG.

²⁰⁷ *Walter/Mayer/Kucsko-Stadlymayer*, Verfassungsrecht¹⁰ Rz 699, S 340 f mit Verweis auf VfGH 06.10.2006, G 151/05.

²⁰⁸ *Jahnel*, Handbuch Datenschutzrecht, 9/12 mit Verweis auf VfGH 04.12.2006, V 22/05 VfSlg 18.021/2006 sowie *Drobesh/Grosinger*, Datenschutzgesetz, Anm zu § 38 Abs 3, 254 und die aA *Dohr/Pollirer/Weiss/Knyrim*, DSG², § 38 Anm 3, 262. Auch in *Pollirer/Weiss/Knyrim*, DSG (2010) § 38 Anm 3 findet sich zu § 38 Abs 3 die Anmerkung „Eine Missachtung des Anhörungsrechts bliebe sanktionslos“.

²⁰⁹ VfGH 04.12.2006, V 22/05.

²¹⁰ Vgl va VfGH 04.12.2006, V 22/05, unter „II., 2.1.“.

Ansicht des VfGH die Gesetzwidrigkeit der Verordnung zur Folge hat. Nicht erwähnt wird hierbei, dass die Verordnung im vorliegenden Fall auch noch mit einer weiteren Gesetzwidrigkeit behaftet war. Sie wurde nämlich entgegen § 5 des Kärntner Ortsbildpflegegesetzes erlassen.

Ob die Nichtbeachtung des Anhörungsrechtes alleine bereits genügt hätte, lässt sich mE nicht zweifelsfrei feststellen. Die erwähnten Kommentare verbreiten ein nur vermeintlich klares Bild. So hat der VfGH schon in der Vergangenheit angenommen, dass „kleinere“ Verstöße gegen Formvorschriften unbeachtlich sein sollen.²¹¹ Diese Ansicht wurde in der Literatur kritisiert.²¹² Andererseits erkannte der VfGH bereits, dass das individuelle Anhörungsrecht von betroffenen Grundeigentümern²¹³ nicht durch Auflage des Planentwurfs im Gemeindeamt ersetzt werden kann.²¹⁴ So werden Anhörungsrechte im Baurecht oder in Raumplanungsgesetzen in der Rsp des VfGH nicht mehr als „kleinere“ Verstöße gegen Formvorschriften gesehen.

Inwieweit die Nichtbeachtung des Anhörungsrechtes der DSK mit dem individuellen Anhörungsrecht betroffener Grundeigentümer vergleichbar ist, ist die wesentliche Frage, um die Ansicht des VfGH prognostizieren zu können. Die genaue Kenntnis der Rsp ist daher unerlässlich, um Leitlinien für kommende Entscheidungen zu erarbeiten.

Dass somit der VfGH bei der bloßen Nichtbeachtung des Anhörungsrechtes der DSK die Gesetzwidrigkeit der VO ausspricht, ist bei der vorliegenden Rsp meiner Meinung nach nicht zweifelsfrei anzunehmen. Inwieweit dies praktisch relevant sein könnte, ist schwer nachzuvollziehen.

Pflichten der Mitglieder der Datenschutzkommission:

- Schaffung einer Geschäftsordnung

„Die DSK hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied).“²¹⁵

Zurecht kritisieren *Pollirer/Weiss/Knyrim*, dass obwohl die DSK eine gerichtsähnliche Organisation darstellt, deren GO nicht veröffentlicht wird.²¹⁶

²¹¹ VfGH 07.12.1994, B 331/94.

²¹² Vgl. v.a. *Walter/Mayer/Kucsko-Stadlymayer*, Verfassungsrecht¹⁰ Rz 1109, S 519.

²¹³ Vgl. § 27 Abs 2 erster Satz Stmk RaumOG 1974, LGBl Nr 127/1974 idF LGBl Nr 59/1995.

²¹⁴ VfGH 11.03.2004, V 126/03.

²¹⁵ § 38 Abs 1 DSG.

²¹⁶ *Pollirer/Weiss/Knyrim*, DSG (2010) § 38 Anm 1.

- Erstellung eines Datenschutzberichtes

Spätestens alle zwei Jahre hat die DSK einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Dieser ist dem Bundeskanzler zur Kenntnis zu übermitteln.²¹⁷

- Veröffentlichungspflicht

Die DSK hat ihre Entscheidungen, welche von grundsätzlicher Bedeutung für die Allgemeinheit sind, unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.²¹⁸ Diese Veröffentlichung finden sich in der ZfV und im Internet unter <http://www.ris.bka.gv.at/dsk> sowie auf der Webseite der DSK²¹⁹.

Klage der Europäischen Kommission gegen die Republik Österreich:

In der am 22. Dezember 2010 eingereichten Klage der Europäischen Kommission gegen die Republik Österreich²²⁰ zur Frage der Unabhängigkeit der österr DSK stellte die Europäische Kommission folgende zwei Anträge:

„1. Die Republik Österreich hat gegen ihre Verpflichtungen aus Artikel 28 Absatz 1 Satz 2 der Richtlinie 95/46/EG verstoßen, weil die in Österreich bestehende Rechtslage bezüglich der als Datenschutzkontrollstelle eingerichteten Datenschutzkommission nicht das Kriterium der völligen Unabhängigkeit erfüllt.

2. Die Republik Österreich trägt die Kosten des Verfahrens.“²²¹

Als Klagegründe und wesentliche Argumente wurden angeführt, dass die österr DSK organisatorisch eng mit dem Bundeskanzleramt verbunden sei, da diese die Dienstaufsicht über die Mitarbeiter der DSK ausübe und auch für deren materielle Ausstattung verantwortlich sei.²²² „Zudem obliege die Leitung der Datenschutzkommission einem Verwaltungsbeamten des Bundeskanzleramts, der auch während dieser Tätigkeit an Weisungen

²¹⁷ Vgl § 38 Abs 4 DSG.

²¹⁸ § 39 Abs 4 DSG.

²¹⁹ <http://www.dsk.gv.at> (Stand: 18.08.2013).

²²⁰ Vgl Klage in der Rechtssache C-614/10.

²²¹ Klage in der Rechtssache C-614/10, unter „Anträge“.

²²² Klage in der Rechtssache C-614/10, unter „Klagegründe und wesentliche Argumente“.

seines Dienstherrn gebunden ist und dessen Dienstaufsicht unterliegt.“²²³ Dies führe zu offensichtlichen Loyalitäts- und Interessenkonflikten.

Als problematisch wurde nach Ansicht der Europäischen Kommission auch angesehen, dass der Bundeskanzler gegenüber der DSK ein umfassendes Aufsichts- und Unterrichtsrecht habe, obwohl dieser selbst der Kontrolle der DSK unterliege. Dadurch könne er sich jederzeit und ohne konkreten Anlass über alle Gegenstände der Geschäftsführung der DSK informieren, wodurch die Gefahr bestehe, dass dieses Recht zur politischen Einflussnahme genutzt werden könne.

Mit Urteil vom 9. März 2010²²⁴ hat der EuGH festgestellt, dass die Datenschutzaufsicht im nicht-öffentlichen Bereich in Deutschland nicht den in der EG-Datenschutzrichtlinie 95/46 festgelegten Anforderungen an die völlige Unabhängigkeit genügt. Die deutschen Datenschutzbeauftragten des Bundes und der Länder haben daraufhin auf ihrer 79. Konferenz eine Entschließung²²⁵ gefasst und sich darin für einen effektiven Datenschutz ausgesprochen, der eine unabhängige Datenschutzkontrolle braucht.

Der Europäische Datenschutzbeauftragte (EDSB) hat mit Schriftsatz, der am 24. März 2011 bei der Kanzlei des Europäischen Gerichtshofs eingegangen ist, beantragt, als Streithelfer in der Rechtssache C-614/10 – also im Verfahren gegen die Republik Österreich – zur Unterstützung der Anträge der Europäischen Kommission zugelassen zu werden. Ebenso hat die Bundesrepublik Deutschland mit Schriftsatz, der am 18. April 2011 (E-Mail vom 14. April 2011) bei der Kanzlei des Europäischen Gerichtshofs eingegangen ist, beantragt, als Streithelfer in der Rechtssache C-614/10 zur Unterstützung der Anträge der Republik Österreich zugelassen zu werden. Beides wurde mit Beschluss des Präsidenten des Europäischen Gerichtshofs²²⁶ zugelassen und jeweils eine Frist zur schriftlichen Begründung der Anträge gesetzt.

²²³ Klage in der Rechtssache C-614/10, unter „Klagegründe und wesentliche Argumente“.

²²⁴ Rechtssache C-518/07.

²²⁵ Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010.

²²⁶ Zum Antrag der Bundesrepublik Deutschland: Beschluss des Präsidenten des Gerichtshofs vom 18. Mai 2011 in der Rs C-614/10.; zum Antrag des EDSB: Beschluss des Präsidenten des Gerichtshofs vom 7. Juli 2011 in der Rs C-614/10.

Am 3. Juli 2012 erhob Generalanwalt Ján Mazák die Schlussanträge und empfahl darin dem Gerichtshof festzustellen, dass die Republik Österreich Art 28 Abs 1 Unterabs 2 der RL 1995/46/EG verletzt habe. Hierfür nannte er vor allem drei Gründe:

- 1) Das geschäftsführende Mitglied der DSK ist zugleich Bundesbeamter.
- 2) Die Geschäftsstelle der DSK ist in das Bundeskanzleramt eingliedert.
- 3) Bundeskanzler hat ein Unterrichtsrecht gegenüber der DSK.

b) Urteil des EuGH und die Folgen für die DSK

Mit Urteil des EuGH vom 16.10.2012²²⁷ hat die Große Kammer des EuGH entschieden, dass die Republik Österreich „dadurch gegen ihre Verpflichtungen aus Art 28 Abs 1 Unterabs 2 der RL 95/46/EG verstoßen hat, dass sie nicht alle Vorschriften erlassen hat, die erforderlich sind, damit die in Österreich bestehende Rechtslage in Bezug auf die DSK dem Kriterium der Unabhängigkeit genügt, und zwar im Einzelnen dadurch, dass sie eine Regelung eingeführt hat, wonach das geschäftsführende Mitglied der DSK ein der Dienstaufsicht unterliegender Bundesbediensteter ist, die Geschäftsstelle der DSK in das Bundeskanzleramt eingegliedert ist und der Bundeskanzler über ein unbedingtes Recht verfügt, sich über alle Gegenstände der Geschäftsführung der Datenschutzkommission zu unterrichten.“²²⁸

Der EuGH hat sich daher den Schlussanträgen des Generalanwalts inhaltlich angeschlossen.

(1) Gesetzliche Änderungen

Da durch die Verwaltungsgerichtsbarkeitsreform ab 1.1.2014 weitreichende Änderungen im Bereich der Verwaltungsgerichtsbarkeit in Kraft treten, wurde durch die DSG-Novelle 2013 eine „Übergangslösung“ geschaffen. Durch die DSG-Novelle 2014 wird dann gleichzeitig die Verwaltungsgerichtsbarkeitsreform umgesetzt.

DSG-Novelle 2013²²⁹:

Die DSG-Novelle 2013 berücksichtigt die aufgrund des Urteils des EuGH notwendigen Änderungen in den § 37 Abs 2, § 38 Abs 2 und § 61 Abs 9 DSG. Gemäß § 60 Abs 6 DSG traten diese Änderungen mit 1. Mai 2013 in Kraft.

²²⁷ EuGH 16.10.2012, Rs C-614/10.

²²⁸ Vgl Tenor des Urteils des EuGH 16.10.2012, Rs C-614/10.

²²⁹ Vgl BGBl I Nr 57/2013: Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013).

Es wurde normiert, dass die DSK eine Dienstbehörde und Personalstelle ist, zu deren Unterstützung eine Geschäftsstelle eingerichtet ist.²³⁰ Zudem ist gemäß § 37 Abs 2 dritter Satz im Bundesfinanzgesetz die notwendige Sach- und Personalausstattung sicherzustellen. Die Diensthoheit über die Bediensteten der Geschäftsstelle übt der Vorsitzende der DSK aus.

Das Unterrichtsrecht²³¹ wurde dahingehend „konkretisiert“, dass der Vorsitzende der DSK dem Unterrichtsrecht nur insoweit zu entsprechen hat, „als dies nicht der völligen Unabhängigkeit der Kontrollstelle im Sinne von Art 28 Abs 1 UAbs 2 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl Nr L 281 vom 23.11.1995 S 31, widerspricht.“²³²

Es wurde daher die Richtlinienbestimmung in den Gesetzestext aufgenommen; eine Streichung des Unterrichtsrechts wurde nicht vorgenommen. Dies ist mE sehr kritisch zu sehen. Der Rechtsanwender wird durch die vom Gesetzgeber gewählte Umsetzung vor beinahe unlösbare Probleme gestellt. Erforderlich wäre die Normierung gewesen, in welchen Fällen das Unterrichtsrecht der völligen Unabhängigkeit iSd RL 95/46/EG widerspricht. ME hat der Gesetzgeber festgestellt, dass das Unterrichtsrecht tatsächlich in einem Widerspruch zur völligen Unabhängigkeit steht und wollte gleichzeitig das Unterrichtsrecht nicht abschaffen. Die sich dadurch eröffnenden Probleme für den Rechtsanwender sind unzumutbar und werden wohl erst durch die DSGVO-Novelle 2014 beseitigt werden.

Die dem Urteil des EuGH zu entnehmende Feststellung, dass die Geschäftsstelle nicht in das Bundeskanzleramt eingegliedert sein sollte und dass das geschäftsführende Mitglied nicht zugleich ein der Dienstaufsicht unterliegender Bundesbediensteter sein sollte, wurde sowohl durch den erwähnten § 37 Abs 2 als auch § 61 Abs 9 DSGVO entsprochen. § 61 Abs 9 sieht vor, dass Bedienstete des Bundeskanzleramtes, die ausschließlich oder überwiegend Aufgaben besorgen, die in den Wirkungsbereich der Geschäftsstelle der DSK fallen, mit Inkrafttreten des BGBl I Nr 57/2013 als Bedienstete der DSK übernommen werden. Welche Bundesbediensteten dies sind, hat der Bundeskanzler mit Bescheid festzustellen. Für

²³⁰ § 37 Abs 2 DSGVO idF BGBl I Nr 57/2013.

²³¹ „Der Bundeskanzler kann sich (...) unterrichten.“ (vgl § 38 Abs 2 DSGVO)

²³² § 38 Abs 2 zweiter Satz DSGVO idF BGBl I Nr 57/2013.

vertraglich Bedienstete gilt dies mit der Maßgabe, dass an die Stelle des Bescheids eine Dienstgebererklärung tritt.²³³

Es fällt auf, dass durch diese Regelung Bedienstete, die nicht ausschließlich oder überwiegend, sondern lediglich in geringem Umfange, Aufgaben des Wirkungsbereichs der Geschäftsstelle der DSK besorgen, nicht erfasst sind. Diese Unterscheidung ist mE in keiner Weise nachvollziehbar, da die Unabhängigkeit und Weisungsfreiheit nicht vom zeitlichen Ausmaß der Beschäftigung mit einem Thema abhängen sollte. Wenn etwa ein Bediensteter der Geschäftsstelle der DSK seine Tätigkeit für die Geschäftsstelle lediglich in einem Umfang von 10 % ausübt, wird er nicht als Bediensteter der DSK übernommen. ME ist die Eingliederung in das Bundeskanzleramt auch dann problematisch, wenn Mitarbeiter nur in geringem Ausmaß für die DSK tätig sind und nicht erst, wenn sie „ausschließlich oder überwiegend Aufgaben besorgen, die in den Wirkungsbereich der Geschäftsstelle der Datenschutzkommission fallen“.

DSG-Novelle 2014²³⁴:

Durch die DSG-Novelle 2014²³⁵ wird die „Datenschutzbehörde“ geschaffen. Die DSK gehört daher mit Ablauf des 31.12.2013²³⁶ der Vergangenheit an. In dieser Dissertation werde ich – entsprechend dem geltenden Recht – den Begriff der DSK verwenden und im folgenden Unterkapitel die wesentlichen Änderungen durch die DSG-Novelle 2014 kurz erläutern.

(2) DSG-Novelle 2014 und die Verwaltungsgerichtsbarkeits-Novelle

Eine Umbenennung einer Behörde alleine bringt keine wesentliche Änderung mit sich. Mit der Umbenennung werden aber gleichzeitig zahlreiche Änderungen vorgenommen, um die von der Verwaltungsgerichtsbarkeits-Novelle²³⁷ verfolgten Ziele zu erreichen, wobei auch einige Bestimmungen zur notwendigen völligen Unabhängigkeit konkretisiert werden. Gemäß § 35 Abs 1 DSG idF BGBl I Nr 57/2013 sind zur Wahrung des Datenschutzes – unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte – die

²³³ Vgl § 61 Abs 9 DSG idF BGBl I Nr 57/2013.

²³⁴ Vgl BGBl I Nr 83/2013

²³⁵ BGBl I Nr 83/2013: Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2014).

²³⁶ § 61 Abs 9 DSG idF BGBl I Nr 83/2013.

²³⁷ BGBl I Nr 51/2012: Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Finanz-Verfassungsgesetz 1948, das Finanzstrafgesetz, das Bundesgesetz, mit dem das Invalideneinstellungsgesetz 1969 geändert wird, das Bundessozialamtsgesetz, das Umweltverträglichkeitsprüfungsgesetz 2000, das Bundesgesetzblattgesetz, das Verwaltungsgerichtshofgesetz 1985 und das Verfassungsgerichtshofgesetz 1953 geändert und einige Bundesverfassungsgesetze und in einfachen Bundesgesetzen enthaltene Verfassungsbestimmungen aufgehoben werden (Verwaltungsgerichtsbarkeits-Novelle 2012).

Datenschutzbehörde und der Datenschutzrat berufen. Ergänzend übt nach § 35 Abs 2 leg cit die Datenschutzbehörde ihre Befugnisse auch gegenüber den in Art 19 B-VG bezeichneten obersten Organen der Vollziehung aus, somit auch gegenüber dem Bundespräsidenten, den Bundesministern und Staatssekretären und den Mitgliedern der Landesregierungen.

Der Leiter der Datenschutzbehörde:

Der Datenschutzbehörde steht ein Leiter vor, der vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt wird.²³⁸ Die Wiederbestellung ist zulässig. Es hat eine Ausschreibung zur allgemeinen Bewerbung zu erfolgen, welche auf der beim BKA eingerichteten Webseite und im Amtsblatt zur Wiener Zeitung auszuschreiben bzw kundzumachen ist. Die fachlichen und persönlichen Voraussetzungen werden in § 36 Abs 2 bis 4 beschrieben (ua Studium der Rechtswissenschaften; ausgezeichnete Kenntnisse des österr Datenschutzrechtes, des Unionsrechtes und der Grundrechte; mindestens fünfjährige juristische Berufserfahrung etc). Der Leiter darf in den letzten zwei Jahren vor seiner Bestellung keine höheren politischen Funktionen²³⁹ ausgeübt haben. Wesentliche Voraussetzung ist auch die Wählbarkeit zum Nationalrat. Zudem ist auch ein Stellvertreter des Leiters zu bestellen.²⁴⁰

Unabhängigkeit der Datenschutzbehörde:

§ 37 DSG idF BGBl I 83/2013 regelt die Organisation und Unabhängigkeit der Datenschutzbehörde. Inhaltlich sind im Vergleich zu den §§ 37 f DSG idF BGBl I 57/2013 (DSG-Novelle 2013) mit dieser Bestimmung keine wesentlichen Änderungen eingeführt worden. Es wird weiterhin auf das Bundesfinanzgesetz verwiesen, das die notwendige Sach- und Personalausstattung sicherzustellen hat. Auch das Unterrichtsrecht des Bundeskanzlers besteht weiterhin mit dem Verweis auf Art 28 Abs 1 UAbs 2 der RL 95/46/EG. Eine mE notwendige Konkretisierung dieses Unterrichtsrechts wäre wünschenswert gewesen.

Anstatt dem spätestens alle zwei Jahre zu erfolgenden Bericht ist nunmehr ein jährlicher Bericht bis spätestens zum 31.3. eines jeden Jahres über die Tätigkeiten des vorangegangenen Kalenderjahres zu erstellen, der dem Bundeskanzler vorgelegt werden muss und in geeigneter

²³⁸ § 36 Abs 1 erster und zweiter Satz DSG idF BGBl I Nr 83/2013.

²³⁹ Vgl § 36 Abs 3 DSG idF BGBl I Nr 83/2013.

²⁴⁰ Vgl § 36 Abs 7 DSG idF BGBl I Nr 83/2013.

Form zu veröffentlichen ist. Dieser Bericht ist sodann vom Bundeskanzler dem Nationalrat und dem Bundesrat vorzulegen.

Instanzenzug:

Durch die Verwaltungsgerichtsbarkeits-Novelle 2012 wird ein (grundsätzlich zweistufiger) Instanzenzug gegen Bescheide von Verwaltungsbehörden eingerichtet. Es werden Landesverwaltungsgerichte, das Bundesverwaltungsgericht und das Bundesfinanzgericht neu geschaffen.

Gegen Bescheide der Datenschutzbehörde sowie wegen Verletzung der Entscheidungspflicht²⁴¹ kann ab 1.1.2014 Beschwerde an das **Bundesverwaltungsgericht** erhoben werden. In Verfahren über Beschwerden gegen Bescheide sowie wegen Verletzung der Entscheidungspflicht in den Angelegenheiten des DSG entscheidet das Bundesverwaltungsgericht durch Senat. Dieser Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer, die jeweils auf Vorschlag der Wirtschaftskammer Österreich und der Bundeskammer für Arbeiter und Angestellte bestellt werden.²⁴²

Gegen Entscheidungen des Bundesverwaltungsgerichts kann ab Inkrafttreten der DSG-Novelle 2014 **Revision beim Verwaltungsgerichtshof** erhoben werden.²⁴³

Bei der Verwaltungsgerichtsbarkeit soll durch die Verwaltungsgerichtsbarkeits-Novelle ein mit der Zivilgerichtsbarkeit vergleichbarer Instanzenzug geschaffen werden. Aus rechtsstaatlicher Sicht ist diese Reform sehr zu loben. Voraussetzung einer unabhängigen (Verwaltungs-)Rechtsprechung sind unabhängige Richter. Es ist daher auf diesen Aspekt besonders zu achten.

²⁴¹ Vgl auch Art 130 B-VG idF BGBl I Nr 51/2012.

²⁴² Vgl § 39 Abs 2 DSG idF BGBl I Nr 83/2013.

²⁴³ Vgl § 40 DSG idF BGBl I Nr 83/2013.

3. Datenschutzrat

a) Geltende Rechtslage

Mitglieder des Datenschutzrates:²⁴⁴

- Vertreter der politischen Parteien

„Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend.“²⁴⁵

Zu den parteipolitischen Vertretern kommen folgende Mitglieder hinzu:

- Je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich,
- zwei Vertreter der Länder²⁴⁶,
- je ein Vertreter des Gemeindebundes und des Städtebundes sowie
- ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

Die Tätigkeit der Mitglieder des Datenschutzrates ist ehrenamtlich, wobei Mitglieder des Datenschutzrates, die außerhalb von Wien wohnen, im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften haben.²⁴⁷

Aufgaben der Mitglieder des Datenschutzrates:

- Beratung der Bundesregierung und der Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Hierzu hat der Datenschutzrat folgende Rechte:²⁴⁸
 - o Beratung über Fragen von grundsätzlicher Bedeutung für den Datenschutz;

²⁴⁴ Vgl § 42 DSG.

²⁴⁵ § 42 Abs 1 Z 1 DSG.

²⁴⁶ Diese werden in der Praxis durch einen Beschluss der Landeshauptleutekonferenz nominiert – vgl *Pollirer/Weiss/Knyrim*, DSG (2010) § 42 Anm 2.

²⁴⁷ § 42 Abs 6 DSG.

²⁴⁸ Vgl § 41 Abs 2 Z 1 bis 6 DSG.

- Stellungnahme zu Gesetzesentwürfen der Bundesministerien, soweit diese datenschutzrechtlich von Bedeutung sind;
 - Stellungnahme zu Vorhaben von Auftraggebern des öffentlichen Bereichs, soweit diese datenschutzrechtlich von Bedeutung sind;
 - Bei Auftraggebern des öffentlichen Bereichs: Recht auf Auskünfte und Berichte sowie die Einsicht in Unterlagen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
 - Recht, von der DSK Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen;²⁴⁹
 - Aufforderung an Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung, die aus datenschutzrechtlicher Sicht Anlass zu Bedenken, zumindest aber Anlass zur Beobachtung geben;
 - Mitteilung der Beobachtungen, Bedenken und allfälliger Anregungen zur Verbesserung des Datenschutzes in Österreich an die Bundesregierungen und die Landesregierungen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.
- Diverse Anhörungs- und Informationsrechte in verschiedenen Materiengesetzen.²⁵⁰

Nach der Systematik des DSG ist der Datenschutzrat als Kontrollorgan eingerichtet.²⁵¹ Gemäß Art 28 der Datenschutzrichtlinie ist für eine Kontrollstelle bei der Ausarbeitung von datenschutzrechtlichen Rechtsverordnungen oder Verwaltungsvorschriften zwingend ein Anhörungsrecht vorgesehen.²⁵² Dieses besteht nach dem Wortlaut des § 41 Abs 2 DSG zumindest hinsichtlich der Landesregierungen nur auf deren Ersuchen. „Die in Art 28 Abs 3 vorgesehenen Untersuchungsbefugnisse und wirksamen Einwirkungsbefugnisse bestehen nur

²⁴⁹ Diese Ziffer (Z 4a) wurde durch BGBl I Nr 133/2009 neu eingefügt. Diese Auskünfte sind auf den in dieser Bestimmung genannten Zweck („rechtspolitische Fragen des Datenschutzes“) beschränkt und umfassen daher idR keine personenbezogenen Daten von BeschwerdeführerInnen – vgl *Pollirer/Weiss/Knyrim*, DSG (2010) § 41 ErläutRV 2010 zu Abs 2 Z 4a.

²⁵⁰ Vgl etwa § 31a Abs 4 ASVG (ELSY – elektronisches Verwaltungssystem der Sozialversicherung), BGBl 1986/164 idF BGBl I Nr 112/2007: § 10 StAG (Einsatz besonderer Ermittlungsmaßnahmen im Ermittlungsverfahren, die gerichtlich bewilligt wurden), ausdrückliche Anhörungsrechte in § 16b MeldeG und § 8 Abs 2 BStatG) et altera – vgl *Jahnel*, Handbuch Datenschutzrecht, 9/23.

²⁵¹ Vgl § 35 DSG.

²⁵² Vgl zur Entstehung der Richtlinie 1995/46/EG: *Graf*, Datenschutzrecht im Überblick² (2010) 13 f.

teilweise, ein eigenes Klagerecht oder Anzeigerecht bei Verstößen gegen datenschutzrechtliche Bestimmungen ist nicht vorgesehen.“²⁵³

Die Tätigkeiten des Datenschutzrates waren in der Vergangenheit für Außenstehende kaum nachvollziehbar.²⁵⁴ Seit September 2007 sind die Stellungnahmen des Datenschutzrates auf der Webseite des BKA²⁵⁵ nachlesbar. Neben den Stellungnahmen finden sich auf der Webseite des BKA unter „Fachinhalte – Datenschutz – Datenschutzrat“ auch Informationen zu den Aufgaben und Mitgliedern des Datenschutzrates.²⁵⁶ Die Webseite der DSK verweist unter „Links – Datenschutzbehörden“ auf die Inhalte über den Datenschutzrat auf der Webseite des Bundeskanzleramtes.²⁵⁷

b) DSGVO-Novelle 2014

Die DSGVO-Novelle 2014 brachte im Zusammenhang mit dem Datenschutzrat nur wenige Änderungen. Zu erwähnen ist in diesem Zusammenhang, dass der ursprünglich geplante „Fachbeirat“²⁵⁸ letztlich nicht Bestandteil der DSGVO-Novelle 2014 wurde. Laut Ausschussbericht ist der Fachbeirat, der als Unterstützung der Datenschutzbehörde tätig sein sollte, entfallen, um jeglichen Zweifel an der Unabhängigkeit der Datenschutzbehörde zu vermeiden. Durch die Änderungen des § 41 Abs 2 Z 1 im Rahmen der DSGVO-Novelle 2014 sollte klargestellt werden, „dass der Datenschutzrat im Rahmen seiner bestehenden Zuständigkeit, Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen zu können, auch Gutachten erstellen oder in Auftrag geben kann.“²⁵⁹

Im Unterschied zur vorhergehenden Regelung des § 44 Abs 6 DSGVO, wonach Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, berechtigt waren, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse (ohne Stimmrecht) teilzunehmen, ist nach der neuen Regelung des § 44 Abs 6 DSGVO²⁶⁰ lediglich der Leiter der Datenschutzbehörde zur Teilnahme an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse berechtigt.

²⁵³ *Jahnel*, Handbuch Datenschutzrecht, 9/28.

²⁵⁴ *Jahnel*, Handbuch Datenschutzrecht, 9/28 zum Zeitpunkt Dezember 2009.

²⁵⁵ <http://www.bundeskanzleramt.at> (Stand: 18.08.2013).

²⁵⁶ <http://www.bundeskanzleramt.at/site/6417/default.aspx> (Stand: 18.08.2013).

²⁵⁷ Vgl <http://www.dsk.gv.at/site/6211/default.aspx> (Stand: 18.08.2013).

²⁵⁸ Vgl § 39 des Gesetzestextes der Regierungsvorlage, 2168 d Beilage, XXIV. GP.

²⁵⁹ Ausschussbericht, 2268 d Beilage, XXIV. GP, Seite 2, zu den Z 9 und 10.

²⁶⁰ § 44 DSGVO idF BGBl I Nr 83/2013.

Den durchgeführten Änderungen entsprechend wird die Verschwiegenheitsverpflichtung in § 44 Abs 8 DSG auf den Leiter der Datenschutzbehörde und die zugezogenen Sachverständigen erweitert²⁶¹; die Mitglieder der Datenschutzkommission werden künftig – da sie nicht mehr teilnehmen können – nicht mehr erwähnt.²⁶²

²⁶¹ Vgl § 44 Abs 8 DSG idF BGBl I Nr 83/2013.

²⁶² Vgl dazu die derzeit geltende Rechtslage: § 44 Abs 8 DSG idF BGBl I Nr 57/2013.

F. SWIFT

SWIFT steht für “Society for Worldwide Interbank Financial Telecommunication”²⁶³ und ist eine 1973 gegründete, internationale Genossenschaft der Geldinstitute, die ein Telekommunikationsnetz für den Nachrichtenaustausch zwischen den Mitgliedern betreibt.²⁶⁴ Mehr als 10.000 Bankorganisationen, Sicherheitsinstitutionen und andere Firmenkunden in mehr als 210 Ländern wickeln täglich mehrere Millionen standardisierte Finanznachrichten über SWIFT ab.²⁶⁵

SWIFT ermöglicht den Kunden Finanztransaktionen zu automatisieren und zu standardisieren, wodurch Kosten verringert, operationelle Risiken reduziert und Ineffizienzen von Abläufen vermieden werden sollen. Diese Aktivität bedingt den sicheren Austausch von gesetzlich geschützten Daten während gleichzeitig Vertraulichkeit und Vollständigkeit gewahrt werden müssen.²⁶⁶ Der Hauptsitz von SWIFT befindet sich in Belgien. Es bestehen Niederlassungen in den bedeutendsten Weltfinanzzentren sowie in diversen Entwicklungsmärkten.

SWIFT hält weder Fonds noch verwaltet es Bankkonten im Interesse von Kunden oder speichert Finanzinformationen auf einer laufend aktualisierten Grundlage. SWIFT verwendet ein „geschlossenes“ Netzwerk, dh es werden dedizierte Leitungen (Standleitungen) verwendet und die Verwaltung erfolgt von einer zentralen Stelle, die Kontrolle über den Netzverkehr hat.²⁶⁷

SWIFT teilt sich in drei Regionen, die mit großer Autonomie sehr selbstständig arbeiten:

- The Americas Region – Region Amerika
- The Asia Pacific Region – Region Asien und Pazifik
- The EMEA Region – Region **E**uropa, **M**ittlerer **O**sten (**M**iddle **E**ast) und **A**frika²⁶⁸

²⁶³ http://www.swift.com/about_swift/index.page – About SWIFT – übersetzt aus dem Englischen (Stand: 18.08.2013).

²⁶⁴ *Birnbauer*, Das Aktienrechts-Änderungsgesetz 2009 (AktRÄG 2009) – Auszüge im Überblick, ÖRPfI 2010 H 2, 33 (34).

²⁶⁵ Vgl http://www.swift.com/about_swift/index.page? – About SWIFT – übersetzt aus dem Englischen (Stand: 18.08.2013).

²⁶⁶ <http://www.swift.com/info?lang=en> – Company information – übersetzt aus dem Englischen (Stand: 18.08.2013).

²⁶⁷ *Hänni/Jans*, Wie sicher ist das Internet? Die Auswirkungen der Vernetzung auf die Informatik-Sicherheit, VWT 1996 Heft 4, 21 (22).

²⁶⁸ http://www.swift.com/about_swift/company_information/leadership_council.page?lang=en – Company information – Organisational structure – übersetzt aus dem Englischen (Stand: 18.08.2013).

Es gibt mehrere Gruppen²⁶⁹:

- Die **Marketing-Gruppe** entwickelt marktsegmentspezifische Lösungen, die die Bedürfnisse der Kunden decken. Sie führt das Produktportfolio fokussiert auf Produktvereinfachung, Benutzerfreundlichkeit und reduzierte Gesamtkosten der Investition auf den Lebenszyklus hinweg betrachtet. Die Marketing-Gruppe ist auch verantwortlich für Standards (eine Schlüsselkomponente des Wertversprechens von SWIFT), Produktinnovationen, Partnermanagement und „Integration Services & Developer Support.“
- Die **IT-Gruppe** ist wesentlich für das alltägliche Geschäft. Die Gruppe verwaltet und überwacht die von den Kunden benutzten Dienstleistungen inklusive dem Betrieb der SWIFT-Zentren und dem globalen Netz. Sie bietet eine große Bandbreite an Instrumenten und Services, die das tägliche Zusammenspiel zwischen den Geschäftsbereichen der Kunden und SWIFT ermöglichen und entwickelt alle Produkte, Applikationen und Technologieplattformen. Die IT-Gruppe ist auch verantwortlich für die Grundstruktur der Sicherheitskontrolle für das Unternehmen SWIFT.
- Die **Finanz- und Verwaltungsgruppe** ist verantwortlich für das Finanzmanagement, Unternehmensplanung, Überwachung der Unternehmensleistung, die Fakturierung, das Beschaffungswesen, die Logistik und allgemeine Verwaltungsdienstleistungen sowie das Einvernehmen mit den Mitbewerbern und deren Angebote. Die Finanz- und Verwaltungsgruppe ist auch verantwortlich für die Preisbildung.

²⁶⁹ Vgl zu Gruppen: http://www.swift.com/about_swift/company_information/leadership_council.page? – Company information – Organisational structure – übersetzt aus dem Englischen (Stand: 18.08.2013).

IV. Informationsverbundsysteme

In diesem Kapitel werde ich einzelne Informationsverbundsysteme vorstellen. Die Informationsverbundsysteme sind für den Datenaustausch von besonderer Bedeutung, insbesondere im Finanzdienstleistungsbereich. Sie ermöglichen einen sehr plastischen Einstieg in diese Thematik, bevor eine theoretische Vertiefung im Bereich des Datenaustausches geschieht.

Nach einem Überblick über Informationsverbundsysteme werde ich mit einem nicht aus dem Finanzdienstleistungsbereich stammenden Informationsverbundsystem, dem Zentralen Melderegister, beginnen, da dieses gesetzlich geregelt wurde und somit keiner Vorabkontrolle durch die DSK unterliegt. Zudem sind beim zentralen Melderegister die (staatlichen) Meldebehörden und nicht private Institutionen wie etwa der KSV 1870²⁷⁰ datenschutzrechtliche Auftraggeber. Anschließend werde ich auf die im Finanzdienstleistungsbereich besonders bedeutsamen Informationsverbundsysteme „Warnliste der österreichischen Banken“ und „Kleinkreditevidenz“ sowie „Mobilfunkverträge und Bonitätsdatenbanken“ eingehen. Schließlich folgt ein Exkurs zum Thema „Bank AGB 2000“.

A. Informationsverbundsysteme im Bankenbereich

1. Allgemeines

Daten werden vor allem durch Informationsverbundsysteme ausgetauscht. Informationsverbundsysteme sind in § 4 Z 13 DSG definiert. Dort heißt es:

Z 13: „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;

Da Informationsverbundsysteme strukturoffen sind, dh „dass im Vorfeld nicht bekannt ist, wann es zu welcher Übermittlung kommt“²⁷¹, stehen sie in einem prinzipiellen Spannungsverhältnis zu den Datenverwendungsgrundsätzen, die in § 6 DSG geregelt sind.

²⁷⁰ Kreditschutzverband von 1870.

²⁷¹ Reimer in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 566.

Ein Rundschreiben²⁷² des Bundeskanzleramtes-Verfassungsdienst (BKA-VD) nennt etwa Informationsverbundsysteme im öffentlichen Bereich, die gesetzlich vorgesehen sind. Eingriffe in das Grundrecht auf Datenschutz sind daher nur zulässig, „wenn sie – bei Verwendung von Informationsverbundsystemen – auf einer gesetzlichen Grundlage beruhen“²⁷³, wobei hierbei Bezug auf den hoheitlichen Bereich genommen wird. Zur Passivlegitimation bei Informationsverbundsystemen hat der OGH ausgesprochen, dass sich der Lösungsanspruch nach § 28 Abs 2 DSGVO und andere Betroffenenrechte in einem Informationsverbundsystem ausschließlich gegen den datenschutzrechtlichen Auftraggeber richten.²⁷⁴ Der Betreiber eines Informationsverbundsystems, der auch teilnehmender Auftraggeber ist, aber nicht den konkreten Datensatz geliefert hat, ist somit nicht passivlegitimiert.²⁷⁵ Zudem reicht ein bloß „logisches Löschen“ nicht aus. Das Lösungsgebot ist nicht erfüllt, wenn die Datenorganisation so verändert wird, dass ein „gezielter Zugriff“ auf die betreffenden Daten nicht mehr möglich ist.²⁷⁶

2. Hoheitliches und nicht hoheitliches Handeln

Reimer weist in seinen Ausführungen darauf hin, dass sowohl der Gesetzesvorbehalt nach Art 18 B-VG als auch jener nach § 1 Abs 2 DSGVO ausschließlich auf hoheitliches Handeln abstellen.²⁷⁷ Die Einrichtung von Informationsverbundsystemen im nicht-hoheitlichen Bereich würden daher keiner ausdrücklichen gesetzlichen Grundlage bedürfen. Informationsverbundsysteme zu nicht-hoheitlichen Zwecken unterliegen seiner Meinung nach aber „den strengen Registrierungsbestimmungen des DSGVO, dh der Vorabkontrolle gemäß § 18 DSGVO“²⁷⁸. Auf die Vorabkontrolle werde ich an späterer Stelle noch genauer eingehen.²⁷⁹ Bei der gesetzlichen Regelung ist insbesondere die Rollenverteilung zu normieren. Darunter wird verstanden, wer Auftraggeber, wer Dienstleister und wer Betreiber des Systems ist.²⁸⁰

²⁷² Bundeskanzleramt-Verfassungsdienst, Rundschreiben zur legislativen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz, BKA-810.016/0001-V/3/2007, S 12 f, <http://www.bka.gv.at/DocView.axd?CobId=29801> (Stand: 18.08.2013).

²⁷³ *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 566.

²⁷⁴ OGH 19.05.2010, 6 Ob 2/10b.

²⁷⁵ Vgl *Bollenberger/Kellner*, OGH 19.05.2010, 6 Ob 2/10b, ÖBA 2010, 853 (853 ff).

²⁷⁶ Vgl OGH 15.04.2010, 6 Ob 41/10p.

²⁷⁷ Vgl *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 566.

²⁷⁸ *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 566.

²⁷⁹ Vgl IV.C.3.a) Exkurs: Vorabkontrolle gem § 18 DSGVO.

²⁸⁰ Bundeskanzleramt-Verfassungsdienst, Rundschreiben zur legislativen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz, BKA-810.016/0001-V/3/2007, Seite 12, <http://www.bka.gv.at/DocView.axd?CobId=29801> (Stand: 18.08.2013).

Zusätzlich wird es im nicht-hoheitlichen Bereich notwendig sein, dass die Auftraggeber und der Betreiber im Innenverhältnis vertraglich Vorkehrungen für die Wahrnehmung der Betreiberpflichten treffen, wobei die diesbezüglichen Vorkehrungen bzw Vereinbarungen nicht der DSK vorgelegt werden müssen.²⁸¹

3. Anwendungsbereiche von Informationsverbundsystemen

Informationsverbundsysteme werden im Bankenbereich für ganz unterschiedliche Zwecke eingesetzt. Zu nennen sind vor allem folgende Bereiche:²⁸²

- Darstellung der Geschäftsentwicklung,
- Sammlung der Adress- und Kontaktdaten von Kunden,
- Beurteilung der Kreditwürdigkeit von Kunden sowie
- Innere Organisation (zB Ausbildungsmaßnahmen für Arbeitnehmer).

²⁸¹ *Duschanek/Rosenmayr-Klemenz*, DSG 2000, 153.

²⁸² Vgl *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 567 mit Verweis auf *Oberndorfer/Trybus*, Informationsverbundsysteme und Datenschutz am Beispiel europäischer Bankengruppen, *ÖZ/2007*, 14.

B. Zentrales Melderegister

1. Begriff

Beim zentralen Melderegister handelt es sich um ein Informationsverbundsystem iSd § 4 Z 13 DSGVO.²⁸³ Gemäß § 16 Abs 2 MeldeG²⁸⁴ sind die Meldebehörden die datenschutzrechtlichen Auftraggeber des Zentralen Melderegisters. Das Bundesministerium für Inneres führt sowohl die Funktion des Betreibers gemäß § 50 DSGVO als auch die eines Dienstleisters im Sinne des § 4 Z 5 DSGVO für diese Datenanwendung aus.

Mit Ausnahme der Angaben zum Religionsbekenntnis haben die Meldebehörden dem Bundesminister für Inneres für die Zwecke des Zentralen Melderegisters ihre Meldedaten samt allenfalls bestehenden Auskunftssperren sowie zugehörigen Abmeldungen zu überlassen.²⁸⁵

Das Zentrale Melderegister hat seit 1.3.2002 im österreichischen Bundesministerium für Inneres den Echtbetrieb aufgenommen, wofür die Meldebehörden zur Datenübermittlung verpflichtet wurden.²⁸⁶

2. Beinhaltete Daten

„Das zentrale Melderegister ist insofern ein öffentliches Register, als der Hauptwohnsitz eines Menschen oder jener Wohnsitz, an dem dieser Mensch zuletzt mit Hauptwohnsitz gemeldet war, abgefragt werden kann, wenn der Anfragende den Menschen durch Vor- und Nach- oder Familiennamen sowie zumindest ein weiteres Merkmal, wie etwa das wirtschaftsbereichsspezifische Personenkennzeichen (§ 14 des E-Government-Gesetzes), Geburtsdatum, Geburtsort oder einen bisherigen Wohnsitz, im Hinblick auf alle im ZMR verarbeiteten Gesamtdatensätze eindeutig bestimmen kann.“²⁸⁷

Die Gesamtheit der Meldedaten eines bestimmten Menschen, mögen diese auch mehrere Unterkünfte betreffen, bildet den Gesamtdatensatz.²⁸⁸

Das MeldeG kennt Meldedaten und Identitätsdaten.

²⁸³ Vgl § 16 Abs 2 MeldeG.

²⁸⁴ BGBl Nr 9/1992, zuletzt geändert durch BGBl I Nr 16/2013: Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG).

²⁸⁵ Vgl § 16 Abs 2 MeldeG.

²⁸⁶ *Bachmann in Bachmann et altera*, *Besonderes Verwaltungsrecht*⁸ (2010), 166.

²⁸⁷ § 16 Abs 1 Satz 1 MeldeG.

²⁸⁸ § 16a Abs 2 Satz 2 MeldeG.

Melddaten sind sämtliche festgehaltenen personenbezogenen Daten auf²⁸⁹

- dem Meldezettel (§ 9),
- dem Gästebuch (§ 10) oder
- der Hauptwohnsitzbestätigung (§ 19a) sowie
- die Melderegisterzahl (ZMR-Zahl).

Unterschriften sind keine Melddaten.

Identitätsdaten sind²⁹⁰

- die Namen,
- das Geschlecht,
- die Geburtsdaten (Ort, Datum, Bundesland, wenn im Inland gelegen, und Staat, wenn im Ausland gelegen),
- die Melderegisterzahl (ZMR-Zahl) und
- die Staatsangehörigkeit,
- bei Fremden überdies Art, Nummer, Ausstellungsbehörde und Ausstellungsdatum sowie der Staat der Ausstellung ihres Reisedokumentes.²⁹¹

3. Zulässigkeit

Der Bundesminister für Inneres hat durch Verordnung²⁹² Näheres über die Vorgangsweise bei Verwendung der Daten nach § 16 Abs 1 und 2 festzulegen.²⁹³

Jedem Gesamtdatensatz kann zur Sicherung der Unverwechselbarkeit der An- und Abgemeldeten eine Melderegisterzahl (ZMR-Zahl) beigegeben werden, die keine Informationen über den Betroffenen enthält.²⁹⁴

Gemäß § 16 Abs 2 MeldeG sind die Meldebehörden die datenschutzrechtlichen Auftraggeber des Zentralen Melderegisters; das Bundesministerium für Inneres übt sowohl die Funktion des

²⁸⁹ Vgl § 1 Abs 5 MeldeG.

²⁹⁰ Vgl § 1 Abs 5a MeldeG.

²⁹¹ Vgl auch <http://zmr.bmi.gv.at> – Allgemein (Stand: 18.08.2013).

²⁹² Geschehen durch BGBl II Nr 66/2002, zuletzt geändert durch BGBl II Nr 65/2010: Verordnung des Bundesministers für Inneres über die Durchführung des Meldegesetzes (Meldegesetz-Durchführungsverordnung - MeldeV).

²⁹³ § 16 Abs 5 MeldeG.

²⁹⁴ § 16 Abs 4 MeldeG.

Betreibers gemäß § 50 DSGVO als auch die eines Dienstleisters im Sinne des § 4 Z 5 DSGVO für diese Datenanwendung aus.²⁹⁵

Nähere Bestimmungen im Hinblick auf Datensicherheitsmaßnahmen, vor allem auch jene betreffend § 16a MeldeG, wurden vom Bundesminister für Inneres in der MeldeV festgelegt.²⁹⁶

Nach § 30 Abs 6 DSGVO kann die DSK zur Herstellung des rechtmäßigen Zustandes, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach § 30 Abs 6a DSGVO zu treffen sind²⁹⁷, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Dies erfolgte 2003²⁹⁸, wobei damals unklar war, wer Adressat des § 30 Abs 6 DSGVO ist (die Meldebehörden als „Auftraggeber des ZMR“ oder das BMI als „Betreiber gemäß § 50 DSGVO und Dienstleister im Sinne des § 4 Z 5 DSGVO“).

4. Judikatur der österr DSK

Seit Inkrafttreten des DSGVO 2000²⁹⁹ scheinen in der Judikaturdatenbank der DSK³⁰⁰ zehn Textdokumente zum MeldeG auf, wobei sich darunter auch die Empfehlung der DSK vom 9. Mai 2003 befindet.

Die Empfehlungen lauteten:

- Die Eingabe von Vor- und Familienname, des Geburtsdatums des gesuchten Menschen (Meldepflichtigen) und eines weiteren Merkmals durch den Übermittlungsempfänger (sonstiger Abfrageberechtigter) muss zwingend vor der Übermittlung von Daten des in Frage kommenden Menschen (Meldepflichtigen) erfolgen. Durch solche programmtechnische Maßnahmen soll sichergestellt werden, dass bei der Übermittlung von personenbezogenen Daten aus dem ZMR durch Abfrage an sonstige Abfrageberechtigte § 16 Abs 1 MeldeG eingehalten wird.³⁰¹ Der Anfragende muss demnach den Meldepflichtigen eindeutig bestimmen können, wozu die Eingabe des Vor- und Familiennamens, des Geburtsdatums und eines weiteren

²⁹⁵ Vgl § 16 Abs 2 MeldeG.

²⁹⁶ Vgl Meldegesetz-Durchführungsverordnung.

²⁹⁷ „sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs 6a leg cit zu treffen sind“ wurde erst durch das BGBl I Nr 133/2009 gemeinsam mit weiteren Änderungen des § 30 DSGVO und anderen Bestimmungen des DSGVO eingefügt.

²⁹⁸ Empfehlungen der Datenschutzkommission gemäß § 30 Abs 6 vom 9. Mai 2003, Geschäftszahl K213.002/008-DSK/2003.

²⁹⁹ Dies war am 1. Jänner 2000 (vgl § 60 DSGVO).

³⁰⁰ Abrufbar unter <http://ris.bka.gv.at> (Stand: 18.08.2013).

³⁰¹ Empfehlungen der Datenschutzkommission gemäß § 30 Abs 6 DSGVO vom 9. Mai 2003, Geschäftszahl K213.002/008-DSK/2003, erste Empfehlung.

Merkmals erforderlich ist. Durch eine kurz nach den Empfehlungen ausgesprochenen Gesetzesänderung wurde diese eindeutige Bestimmbarkeit insofern abgeändert³⁰², als zusätzlich zum Vor- und Familiennamen nur noch zumindest ein weiteres Merkmal angegeben werden muss. Die Angabe des Vor- und Familiennamens und des Geburtsdatums genügt somit seit 1.3.2004 als „eindeutig bestimmbar“ iSd Bestimmung. Hier wird klar, wie auf Empfehlungen der DSK reagiert werden kann, ohne die Empfehlung zwingend umzusetzen. Durch die Änderung der rechtlichen Grundlagen wurde die Empfehlung der DSK ausgehebelt, was meines Erachtens zu einer weiteren Einschränkung der Persönlichkeitsrechte des Einzelnen führte.

- Durch eine Verordnung möge der Bundesminister für Inneres auf Grundlage der Ermächtigung in § 16a Abs 6 MeldeG den Ablauf einer zulässigen Abfrage aus dem ZMR durch sonstige Abfrageberechtigte innerhalb der Grenzen des § 16 Abs 1 MeldeG regeln.³⁰³
- Die dritte Empfehlung trug dem Bundesminister für Inneres auf, durch geeignete Maßnahmen, insbesondere die Androhung und Einleitung von Verfahren zur Entziehung der Abfrageberechtigung (§ 16a Abs 7 MeldeG) dafür Sorge zu tragen, dass sonstige Abfrageberechtigte die Daten des ZMR ausschließlich für den in § 16a Abs 5 MeldeG umschriebenen Zweck („zur erwerbsmäßigen Geltendmachung oder Durchsetzung von Ansprüchen“) verwenden und ZMR-Daten keinesfalls zur Übermittlung an Dritte zu ermitteln oder neben der Verwendung für eigene, rechtmäßige Zwecke an Dritte zu übermitteln.³⁰⁴ Auch hier erfolgte eine Gesetzesänderung, wodurch ein Teil es § 16a Abs 5 entfiel und ein neuer Absatz 5a eingefügt wurde. Als Strafbestimmung wurde durch BGBl I Nr 10/2004 die Ziffer 8 eingefügt, die festschreibt, dass jemand, der gegen § 16a Abs 5a MeldeG verstößt, eine Verwaltungsübertretung begeht und mit Geldstrafe bis zu EUR 726,00, im Wiederholungsfall mit Geldstrafe bis zu EUR 2.180,00, (dies entspricht etwa der dreifachen Höhe von EUR 726,00) zu bestrafen ist. Auch kann neben der Verhängung einer Geldstrafe über den Entzug der Abfrageberechtigung gemäß § 16a Abs 5 für die Dauer von höchstens sechs Monaten erkannt werden, wenn dies erforderlich erscheint, um den Betroffenen von weiteren gleichartigen Verwaltungsübertretungen

³⁰² Vgl BGBl I Nr 10/2004.

³⁰³ Empfehlungen der Datenschutzkommission gemäß § 30 Abs 6 DSG vom 9. Mai 2003, Geschäftszahl K213.002/008-DSK/2003, zweite Empfehlung.

³⁰⁴ Empfehlungen der Datenschutzkommission gemäß § 30 Abs 6 DSG vom 9. Mai 2003, Geschäftszahl K213.002/008-DSK/2003, dritte Empfehlung.

abzuhalten.³⁰⁵ Die Empfehlung, welche sich an den Innenminister richtete, wurde somit vom Gesetzgeber umgesetzt. Dadurch wurde mehr Klarheit im Meldegesetz geschaffen, was mE sehr zu begrüßen ist.

Die Judikatur bezieht sich auf folgende Bereiche:³⁰⁶

- Zumindest teilweise Verletzung³⁰⁷ oder gänzliche Nichtverletzung³⁰⁸ des Rechts auf **Geheimhaltung schutzwürdiger personenbezogener Daten nach § 1 DSGVO** et altera.
- Genehmigung³⁰⁹ oder Nichtgenehmigung³¹⁰ der Verwendung von Daten des ZMR für **wissenschaftliche Zwecke nach §§ 46 f DSGVO**.
- Verletzung³¹¹ oder Nichtverletzung³¹² des Rechts auf **Auskunft nach § 26 DSGVO**.

5. Vergleichbare Systeme in Deutschland

Gem Art 76 Abs 1 Z 3 GG³¹³ hat die Bundesrepublik Deutschland ua die ausschließliche Gesetzgebung über das Meldewesen. Diese Änderung erfolgte im Gesetz zur Änderung des Grundgesetzes vom 28. August 2006.³¹⁴ Das Melde- und Ausweiswesen wurden hiermit in Art 76 Abs 1 Z 3 GG³¹⁵ zur Bundeskompetenz erhoben. Da bislang keine politische Einigung möglich war, bestehen nach wie vor 16 unterschiedliche landesgesetzliche Regelungen. Es gibt jedoch ein Melderechtsrahmengesetz³¹⁶, das wesentliche Harmonisierungsbestimmungen für die landesgesetzlichen Regelungen enthält. So schreibt etwa § 2 MRRG vor, welche Daten die Meldebehörden im Melderegister zu speichern haben.

Ein neues Bundesmeldegesetz soll dann sowohl die landesgesetzlichen Regelungen als auch das Melderechtsrahmengesetz ersetzen.

³⁰⁵ Vgl § 22 DSGVO idF BGBl I Nr 10/2004.

³⁰⁶ Hierbei wurden die auf der Webseite des österr Bundeskanzleramtes veröffentlichten Bescheide der Datenschutzkommission im Bereich des Meldegesetzes seit 1.1.2000 berücksichtigt, vgl <https://www.ris.bka.gv.at/Dsk/> (Stand: 18.08.2013).

³⁰⁷ DSK 18.05.2000, 120.616/16-DSK/00 und DSK 11.07.2003, K120.629/002-DSK/2003 (beide geprüft nach der Rechtslage vor dem 1.1.2000); DSK 07.06.2005, K121.006/0007-DSK/2005 und DSK 14.04.2010, K121.564/0006-DSK/2010.

³⁰⁸ DSK 18.05.2011, K121.667/0012-DSK/2011.

³⁰⁹ DSK 07.09.2006, K202.047/0009-DSK/2006.

³¹⁰ Es lag hierbei eine Zurückweisung vor, da es sich materiell um die Durchführung einer Kette von Meldeauskünften gemäß § 18 Abs 1 MeldeG handelte, worüber die Meldebehörden zu entscheiden haben – vgl DSK 12.05.2010, K202.088/0003-DSK/2010.

³¹¹ DSK 10.08.2007, K121.275/0007-DSK/2007.

³¹² DSK 18.09.2009, K121.518/0005-DSK/2009.

³¹³ Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2010 (Deutsches BGBl 2010 I, Nr 38, S 944) geändert worden ist (GG).

³¹⁴ Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 (Deutsches BGBl 2006 I, Nr 41, S 2034).

³¹⁵ Vgl Art 1 Z 6 lit a lit aa des Gesetzes zur Änderung des Grundgesetzes.

³¹⁶ Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 19. April 2002 (BGBl 2002 I S 1342), das zuletzt durch Artikel 9 des Gesetzes vom 28. April 2011 (BGBl 2011 I S 678) geändert worden ist (MRRG).

C. Warnliste der österreichischen Kreditinstitute

1. Begriff

Die sogenannte „Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten“ dient dem Gläubigerschutz.³¹⁷

Da es sich bei der Warnliste um ein Informationsverbundsystem iSd § 4 Z 13 und § 50 DSGVO handelt und die Warnliste den Zweck des § 18 Abs 2 Z 3 DSGVO (Auskunftserteilung über die Kreditwürdigkeit der Betroffenen) erfüllt, unterliegt sie der Vorabkontrolle durch die DSK.³¹⁸

Die „Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten“ wurde mit Auflagen in der konsolidierten Fassung der Bescheide K095.014/016-DSK/2001 und K095.014/021-DSK/2001³¹⁹ durch die DSK bewilligt. Der Bescheid der DSK vom 21. September 2001³²⁰ wurde mit Bescheid vom 23. November 2001 gemäß § 68 Abs 2 AVG³²¹ dahingehend abgeändert, dass im vorletzten Satz des ersten Punktes des Bescheidspruchs nach den Worten „nach Eintragung in die Warnliste“ die Worte „aber in engem zeitlichem Zusammenhang mit dieser Eintragung“ eingefügt wurden.

Die konsolidierte Fassung der beiden Bescheide erging an vier österreichische Bankunternehmen. Entscheidend für die normative Wirkung ist gemäß § 21 Abs 2 DSGVO der in der konsolidierten Fassung wiedergegebene Wortlaut der den Teilnehmern des Informationsverbundsystems „Warnliste“ (IVB) erteilten Auflagen.³²²

2. Beinhaltete Daten

In die „Warnliste“ werden Kunden des Auftraggebers bzw deren Bürgen (Garanten und Mitschuldner) eingetragen, wenn

³¹⁷ *Koziol*, OGH 15.12.2005, 6 Ob 275/05t, ÖBA 2006, 530 (533).

³¹⁸ Vgl § 18 Abs 2 DSGVO; *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 567.

³¹⁹ Beide zu Grund liegenden Bescheide (K095.014/016-DSK/2001 und K095.014/021-DSK/2001) wurden für Zwecke des RIS unter K095.014/021-DSK/2001 zusammengezogen – vgl 1. Anmerkung zu DSK 23.11.2001, K095.014/021-DSK/2001.

³²⁰ DSK 21.09.2001, K095.014/016-DSK/2001.

³²¹ BGBl Nr 51/1991 idF BGBl Nr 471/1995: Allgemeines Verwaltungsverfahrensgesetz 1991 – AVG.

³²² Vgl 2. Anmerkung zu DSK 23.11.2001, K095.014/021-DSK/2001.

a) der Kunde sein Konto durch vertragswidrig ausgestellte Schecks oder durch vertragswidrige Verwendung seiner Bankomat- oder Kreditkarte unerlaubt überzogen hat oder

b) eine mit dem Kunden bestehende Konto- bzw Kreditverbindung aufgekündigt bzw fällig gestellt oder in die Rechtsverfolgung übergeben wurde

UND die Forderung innerhalb der im Fälligungsschreiben (Kontoaufkündigungsschreiben) gesetzten Zahlungsfrist nicht vollständig bezahlt wurde, wobei der aushaftende Betrag EUR 1.000,-- übersteigt.³²³

Bevor ein Fälligungsschreiben zugesendet wird, sind der Kunde und allfällige Bürgen in gebührender Weise zu mahnen.³²⁴

Falls vor Ablauf der im Fälligungsschreiben bezeichneten Zahlungsfrist eine Vereinbarung über die Schuld-Tilgung getroffen wird, darf die Eintragung in die Warnliste nicht erfolgen.³²⁵ Sollte erst nach dem Ablauf der Eintragung in die Warnliste, aber in engem zeitlichem Zusammenhang damit, eine solche Vereinbarung geschlossen werden, „ist in der Warnliste ein Vermerk über das Bestehen einer Tilgungsvereinbarung anzubringen“³²⁶.

Für den Fall, dass eine begründete Bestreitung der Forderung dem Grund nach vorliegt, hat der Auftraggeber zu veranlassen, dass dies durch einen Bestreitungsvermerk unverzüglich ersichtlich gemacht wird.³²⁷ Auch die vollständige Bezahlung der Forderung ist unverzüglich in der Warnliste auszuweisen.³²⁸

Sofern rechtskräftig festgestellt wurde, dass die Forderung dem Grunde nach nicht besteht, „hat der Auftraggeber zu veranlassen, dass die Daten des Betroffenen aus der Warnliste unverzüglich gelöscht werden“³²⁹.

Um andere Kreditinstitute über das Vertragserfüllungsverhalten des Betroffenen zu informieren³³⁰, werden die Daten des Betroffenen erst drei Jahre nach vollständiger Bezahlung der Schuld bzw in allen anderen Fällen sieben Jahre nach Tilgung der Schuld aus der Warnliste gelöscht.³³¹

³²³ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 1., Satz 1.

³²⁴ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 1., Satz 2.

³²⁵ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 1., Satz 3.

³²⁶ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 1., vorletzter Satz.

³²⁷ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 4., Satz 1.

³²⁸ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 4., Satz 2.

³²⁹ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 5., Satz 1.

³³⁰ Vgl Rechtssatz zu DSK 23.11.2001, K095.014/021-DSK/2001.

³³¹ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 5., Satz 2.

3. Zulässigkeit

a) Exkurs: Vorabkontrolle gem § 18 DSG

Wie bereits erwähnt, unterliegt die Aufnahme der Verarbeitung der Warnliste aus mehreren Gründen einer Vorabkontrolle.

Maßgebliche Bestimmung ist § 18 DSG, welcher den Vollbetrieb von meldepflichtigen Datenanwendungen regelt. Der Vollbetrieb darf – außer in den Fällen des § 18 Abs 2 leg cit – unmittelbar nach Abgabe der Meldung aufgenommen werden³³²:

Wenn eine Musteranwendung iSd § 19 Abs 2 DSG vorliegt, eine innere Angelegenheit der anerkannten Kirchen und Religionsgesellschaften betroffen ist oder die Verwendung von Daten im Katastrophenfall für die in § 48a Abs 1 genannten Zwecke vorliegt, ist keine Vorabkontrolle notwendig.

Andere meldepflichtige Datenanwendungen dürfen in folgenden Fällen erst nach ihrer Prüfung (Vorabkontrolle) durch die DSK nach den näheren Bestimmungen des § 20 DSG aufgenommen werden³³³:

1. sensible Daten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs 4 DSG sind enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen ist Zweck der Datenanwendung oder
4. die Datenanwendung wird in Form eines Informationsverbundsystems durchgeführt werden.

b) Zulässigkeit der Warnliste

Bei der Warnliste handelt es sich sowohl um die Auskunftserteilung über die Kreditwürdigkeit Betroffener³³⁴, als auch um ein Informationsverbundsystem³³⁵. Der Betrieb der Warnliste bedarf daher der Prüfung (Vorabkontrolle) durch die DSK. Für die Aufnahme des Betriebes können dem Auftraggeber gem § 21 Abs 2 DSG Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit

³³² Vgl § 18 Abs 1 DSG.

³³³ Vgl § 18 Abs 2 DSG.

³³⁴ § 18 Abs 2 Z 3 DSG.

³³⁵ § 18 Abs 2 Z 4 DSG.

dies zur Wahrung der durch das Datenschutzgesetz geschützten Interessen der Betroffenen notwendig ist.³³⁶

Unter „Beinhaltete Daten“³³⁷ wurden bereits die Auflagen für den Bereich der einzutragenden Daten dargelegt.

Weitere Auflagen sind:³³⁸

- Ausdrücklicher Hinweis an den betroffenen Kunden und dessen Bürgen (Garanten und Mitschuldner) im Fälligestellungsschreiben bzw Kontoaufkündigungsschreiben, dass³³⁹
 - o *„er in die Warnliste eingetragen wird, falls innerhalb der in diesem Schreiben gesetzten Zahlungsfrist keine vollständige Zahlung erfolgt oder keine andere Vereinbarung getroffen wird, und, dass*
 - o *es sich bei der Warnliste um eine zu Zwecken des Gläubigerschutzes und der Risikominimierung geführte Liste handelt, aus der die teilnehmenden Banken einen Warnhinweis auf vertragswidriges Kundenverhalten entnehmen können.“*³⁴⁰
- Information des Betroffenen im Fälligestellungs- bzw Kontoaufkündigungsschreiben über Möglichkeit des Kontakts mit dem Auftraggeber oder ab dem Zeitpunkt der Eintragung seiner Daten in die Warnliste auch mit einem Gläubigerschutzverein, insbesondere zur Geltendmachung des Auskunfts-, Richtigstellungs-, Löschungs- oder Widerspruchsrecht gemäß §§ 26, 27 und 28 DSG. Zusätzlich können Rechtsbehelfe nach §§ 30 bis 32 DSG ergriffen werden.³⁴¹
- Neben der Pflicht zur ständigen Aktualisierung, müssen die in der Warnliste enthaltenen Daten mindestens einmal jährlich auf ihre Richtigkeit überprüft werden.³⁴²

³³⁶ Vgl § 21 DSG.

³³⁷ Vgl IV.B.2 Beinhaltete Daten.

³³⁸ Diese sind aus dem Spruch der konsolidierten Fassung der Bescheide K095.014/016-DSK/2001 und K095.014/021-DSK/2001 ersichtlich.

³³⁹ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 2.

³⁴⁰ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 2., a) und b).

³⁴¹ DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 3.

³⁴² DSK 23.11.2001, K095.014/021-DSK/2001, Spruch I, 6.

4. Judikatur der österr DSK

In diesem Teil werde ich jeweils auf die überschaubare Judikatur der österr DSK und, soweit erforderlich, auf die Judikatur des OGH eingehen. Systematische Folgen ziehe ich daraus dann im Kapitel „V. A. Österreichisches Datenschutzgesetz (DSG)“.

Entsprechend der Zuständigkeit der DSK gemäß § 1 Abs 5 DSG³⁴³ sind hauptsächlich Entscheidungen zum Auskunftsbegehren zu finden.³⁴⁴

Die DSK hat zum Teil detaillierte Bescheide zum Inhalt der zu erteilenden Auskunft erlassen³⁴⁵ oder verweist generell auf eine gesetzmäßig zu erteilende Auskunft, inklusive der im Einzelfall relevanten Daten.³⁴⁶ In mehreren Bescheiden wurde das Recht auf Auskunft aus unterschiedlichen Gründen nicht als verletzt angesehen: Keine Identität des Betroffenen und des Beschwerdeführers (Personengesellschaft und Privatperson)³⁴⁷, Anwendungsbereich des SPG³⁴⁸, kein erkennbares Anbringen eines Auskunftsbegehens³⁴⁹ und keine Widersprüche der erteilten Auskünfte³⁵⁰.

Teilweise wurde dem Recht auf Auskunft in folgenden Bereichen stattgegeben: Unzulässigkeit des Einschränkens der Auskunft auf die letzten sechs Monate³⁵¹, Auskunft auch über länger zurückliegende Kontobewegungen, die bereits auf Mikrofilmen archiviert wurden, gegen Kostenersatz³⁵² und zulässiges Auskunftsbegehren im Einzelfall gegenüber der Auftraggeberin – nicht jedoch gegenüber dem Dienstleister³⁵³.

Auch eine Verweisung auf den Zivilrechtsweg wurde mittels Bescheid festgestellt.³⁵⁴

Zudem wurde die DSK aufgefordert, in ein Verfahren vor dem Landesgericht für Zivilrechtssachen Wien (LG ZRS)³⁵⁵ wegen einer Löschungsklage, als Nebenintervenientin gem § 32 Abs 6 DSG einzutreten, was die DSK in einem Bescheid bestätigte.³⁵⁶

³⁴³ § 1 Abs 5 DSG: Gegen *Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. (...)*

³⁴⁴ Hierbei wurden die auf der Webseite des österr Bundeskanzleramtes veröffentlichten Bescheide der Datenschutzkommission im Bereich des Meldegesetzes seit 1.1.2000 berücksichtigt, vgl <https://www.ris.bka.gv.at/Dsk/> (Stand: 18.08.2013).

³⁴⁵ So etwa DSK 03.12.2002, K120.804/016-DSK/2002.

³⁴⁶ DSK 24.11.2010, K121.646/0011-DSK/2010.

³⁴⁷ DSK 07.12.2004, K120.938/0003-DSK/2004.

³⁴⁸ DSK 01.02.2005, K120.637/0001-DSK/2005.

³⁴⁹ DSK 22.10.2008, K121.386/0009-DSK/2008.

³⁵⁰ DSK 19.06.2009, K121.494/0013-DSK/2009.

³⁵¹ DSK 10.08.2007, K121.276/0014-DSK/2007.

³⁵² DSK 25.02.2009, K121.394/0006-DSK/2009.

³⁵³ Zudem war in diesem Fall nicht ersichtlich, dass es sich gegenüber der Zweitbeschwerdegegnerin um ein Auskunftsbegehren handelte. Es war lediglich ein Löschungsbegehren erkenntlich – DSK 27.08.2010, K121.599/0014-DSK/2010.

³⁵⁴ DSK 05.04.2006, K121.136/0004-DSK/2006.

³⁵⁵ Es handelte sich um das Verfahren zu 13 Cg 16/07d, LG ZRS Wien.

³⁵⁶ DSK 27.04.2007, K211.797/0004-DSK/2007.

Zentrale Bestimmung der Judikatur der DSK im Bereich der sog Warnliste ist aufgrund der Zuständigkeit das Auskunftsrecht in § 1 Abs 3 und Abs 4 DSGVO mit den (einfachgesetzlichen) Ausführungsbestimmungen in § 26 DSGVO. § 1 Abs 3 DSGVO behandelt das Recht auf Auskunft und das Recht auf Richtigstellung unrichtiger Daten sowie das Recht auf Löschung unzulässig verarbeiteter Daten. Demnach hat jedermann nach Maßgabe gesetzlicher Bestimmungen³⁵⁷ das „Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden.“³⁵⁸

Davon betroffen sind sowohl personenbezogene Daten zur automationsunterstützten Verarbeitung als auch Daten zur Verarbeitung in manuell, das heißt ohne Automationsunterstützung, geführten Dateien.³⁵⁹

Beschränkungen dieser Rechte sind nur unter den in § 1 Abs 2 DSGVO genannten Voraussetzungen zulässig.³⁶⁰

§ 26 DSGVO regelt als einfachgesetzliche Ausführungsbestimmung³⁶¹ das Recht auf Auskunft. Diese Bestimmung hat idF BGBl I Nr 133/2009 zehn Absätze, wobei Absatz 1 leg cit das Recht auf Auskunft detailliert umschreibt. Diese Bestimmung lautet:

(1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hierfür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche

³⁵⁷ Dies ist als Verweis auf weitere (einfach-)gesetzliche Bestimmungen zu sehen.

³⁵⁸ § 1 Abs 3 Z 1 DSGVO.

³⁵⁹ Vgl § 1 Abs 3 DSGVO.

³⁶⁰ § 1 Abs 4 DSGVO.

³⁶¹ Vgl Pollirer/Weiss/Knyrim, DSGVO (2010) § 26 Anm 2.

*Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.*³⁶²

§ 26 Abs 2 DSG erläutert, wann die Auskunft nicht zu erteilen ist und nennt den Schutz des Auskunftswerbers aus besonderen Gründen oder überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen. Überwiegende öffentliche Interessen werden sodann nicht abschließend³⁶³ aufgezählt.³⁶⁴

Zur Prüfung der Zulässigkeit der Auskunftsverweigerung aus den in § 26 Abs 2 Z 1 bis 5 DSG genannten Gründen ist die DSK nach § 30 Abs 3 DSG, Beschwerdeverfahren gemäß § 31 Abs 4 DSG, zuständig.

Die Absätze 3 bis 10 des § 26 DSG normieren die zumutbare Mitwirkungspflicht des Auskunftswerbers³⁶⁵, zu beachtende Fristen³⁶⁶, das Vorgehen bei Erteilung von Auskünften in den Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind³⁶⁷, die Unentgeltlichkeit der jährlichen Auskunft bzw zulässige Entgeltlichkeit in anderen Fällen³⁶⁸, die Pflicht des Auftraggebers zur Archivierung der Daten über den Auskunftswerber ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen³⁶⁹, das Recht auf Auskunft und dessen Umfang bei öffentlichen Büchern und Registern³⁷⁰ und unterschiedliche Adressaten eines Auskunftsbegehrens und deren Verpflichtung zur Auskunft³⁷¹.

Für Betreiber von Informationsverbundsystemen wird auf § 50 Abs 1 DSG verwiesen, der zusätzlich zu den dort genannten Sonderbestimmungen auf die sinngemäße Anwendung des § 26 Abs 3 bis 10 DSG zurückverweist.

³⁶² § 26 Abs 1 DSG.

³⁶³ Arg. „können“ in § 26 Abs 2 DSG.

³⁶⁴ ZB Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich; Vorbeugung, Verhinderung oder Verfolgung von Straftaten;...

³⁶⁵ Vgl § 26 Abs 3 DSG.

³⁶⁶ § 26 Abs 4 DSG normiert acht Wochen nach Einlangen des Begehrens, innerhalb derer die Auskunft zu erteilen ist oder schriftlich zu begründen ist, warum sie nicht oder nicht vollständig erteilt wird.

³⁶⁷ Vgl § 26 Abs 5 DSG.

³⁶⁸ Vgl § 26 Abs 6 DSG.

³⁶⁹ Vgl § 26 Abs 7 DSG.

³⁷⁰ § 26 Abs 8 und 9 DSG.

³⁷¹ § 26 Abs 10 DSG.

Auch mehrere Bescheide, durch die Informationsverbundsysteme genehmigt wurden³⁷², finden sich in der Rubrik der Judikatur der DSK. Hierbei sind folgende Informationsverbundsysteme zu erwähnen:

- Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Verhalten³⁷³,
- Warnliste der österreichischen Versicherungsunternehmen zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf auffälliges Vermittlerverhalten im Vertrieb³⁷⁴ und die
- Kleinkreditevidenz (Konsumentenkreditevidenz) zum Zweck des Gläubigerschutzes und der Risikominimierung (KKE).³⁷⁵

Vom OGH entschiedene Urteile zum Themenbereich „Warnliste“ sind sehr rar. Im Folgenden werde ich einen kurzen Überblick zu jenen Judikaten des OGH geben, aus welchen Rechtssätze abgeleitet wurden und die für die Entwicklung des Datenschutzrechtes in diesem Bereich von besonderer Bedeutung waren:

1. OGH 15.12.2005, 6 Ob 275/05t et altera:

Gegenstand dieses Verfahrens³⁷⁶ ist die Klage einer Bank gegen einen Rechtsanwalt als Bürge und Zahler für restlich € 15.000 samt Anhang und die Widerklage eines Rechtsanwaltes, mit der er einen Schadenersatz (nach Einschränkung) in Höhe von € 30.000 geltend macht. Grund für den Schadenersatz sei die rechts- und vertragswidrige Eintragung in die „Warnliste der Banken“, durch die er einen Vermögens- und Reputationsschaden erlitten habe.

Das Erstgericht verpflichtete den Beklagten zur Zahlung des im Verfahren 5 Cg 223/02m von der klagenden Bank angesprochenen Restbetrags von €15.000 samt 4 % (gestaffelter) Zinsen und 5 % Verzugszinsen; das Zinsenmehrbegehren wies es (rechtskräftig) ab. Dieses Urteil wurde mit Urteil vom Oberlandesgericht Graz als Berufungsgericht vom 6. Juli 2005, GZ 2 R 96/05p-59, bestätigt, wobei die ordentliche Revision für zulässig erklärt worden ist. Der beklagte Rechtsanwalt ergriff hierauf ordentliche Revision, die jedoch vom OGH als nicht zulässig erachtet wurde.

³⁷² Ergänzend wurden iSd § 21 Abs 2 DSG zahlreiche Auflagen erteilt.

³⁷³ Konsolidierte Fassung: DSK 23.11.2001, K095.014/021-DSK/2001.

³⁷⁴ DSK 21.03.2007, K600.014-010/0002-DVR/2007.

³⁷⁵ Bereits zuvor bestehend, neuerlich als Mustererledigung erlassen durch DSK 12.12.2007, K600.033-018/0002-DVR/2007. Vgl Kapitel „4. C. Kleinkreditevidenz“.

³⁷⁶ OGH 15.12.2005, 6 Ob 275/05t.

Im Verfahren 5 Cg 44/03i verpflichtete das Landesgericht Leoben als Erstgericht³⁷⁷ die dort beklagte Bank zur Zahlung eines Schadenersatzbetrags³⁷⁸ von € 25.000 samt 4 % Zinsen seit 20.2.2003. Das Oberlandesgericht Graz als Berufungsgericht hob mit Beschluss die das Verfahren 5 Cg 44/03i betreffende Entscheidung auf und trug diesem die neuerliche Entscheidung nach Verfahrensergänzung auf. Die dagegen ergangenen Rekurse beider Streitteile wurden vom OLG ebenfalls für zulässig erklärt. Den Rekurs der klagenden Bank erachtete der OGH als zulässig, aber nicht berechtigt. Somit hat das Erstgericht sein Verfahren zu ergänzen, damit dem Bestimmtheitsgebot des § 226 ZPO folgend, die Höhe des begehrten materiellen und immateriellen Schadenersatzanspruch beziffert werden kann.

a) Immaterieller Schaden/Schadenersatz (§ 33 DSGVO):

Der OGH hat mit 6 Ob 275/05t klargestellt, dass bei einer gegen das Datenschutzgesetz verstoßenden Aufnahme eines Rechtsanwalts in die Warnliste der Banken, die Voraussetzung für den Zuspruch eines immateriellen Schadens dem Grunde nach gegeben sind.³⁷⁹

„Die dadurch verbreitete Annahme, der Betroffene sei als Rechtsanwalt kreditunwürdig, untergräbt sein Ansehen bei Klienten und unter Kollegen und ist geeignet, seinen Ruf nachhaltig zu schädigen und sogar seine wirtschaftliche Existenz zu gefährden (*Dohr/Pollirer/Weiss/Knyrim* aaO 227).“³⁸⁰

Die Höhe des immateriellen Schadenersatzes war jedoch nicht bestimmbar, weil der Kläger den als immateriellen Schaden geltend gemachten Betrag noch nicht beziffert hat. Bei der Höhe des immateriellen Schadenersatzes ist auf Umfang und Auswirkungen der Datenverwendung³⁸¹ Bedacht zu nehmen. Auch ist zu beachten, dass der Beklagte durch Nichtzahlung bei Fälligkeit grundsätzlich Anlass für die Aufnahme in die Warnliste gegeben hat und der Verstoß der Beklagten gegen datenschutzrechtliche Bestimmungen (nur) darin bestand, dass sie dem Beklagten keine Möglichkeit geboten hatte, vor Aufnahme in die Warnliste Zahlung zu leisten oder sich dagegen zur Wehr zu setzen.³⁸²

³⁷⁷ Landesgericht Leoben zu 5 Cg 44/03i.

³⁷⁸ Zur Geltendmachung von Schadenersatz im Datenschutzgesetz: § 33 DSGVO.

³⁷⁹ Vgl OGH 15.12.2005, 6 Ob 275/05t.

³⁸⁰ OGH 15.12.2005, 6 Ob 275/05t mit Verweis auf *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 33, 227.

³⁸¹ OGH 15.12.2005, 6 Ob 275/05t mit Verweis auf *Berka/Höhne/Noll/Polley*, Mediengesetz², Vor §§ 6-8a MedienG Rz 43 f, S 73 f.

³⁸² Vgl OGH 15.12.2005, 6 Ob 275/05t.

Auch in einer anderen Entscheidung³⁸³ stellte der OGH klar, dass bloßstellen iSd § 33 Abs 1 zweiter Satz DSGVO bedeutet, dass Tatsachen enthüllt werden, die den Betroffenen aus Sicht Dritter herabsetzen und sein Ansehen untergraben³⁸⁴, es muss sich daher nicht um Daten aus dem „höchstpersönlichen Lebensbereich“ handeln – „mögen auch die Datenarten dem höchstpersönlichen Lebensbereich eines Menschen zugehören“³⁸⁵. Ebenso wurde entschieden, dass auch eine begrenzte Öffentlichkeit oder ein begrenzter Kreis an Personen nicht ausschließt, dass durch die öffentlich zugängliche Verwendung dieser Daten schutzwürdige Geheimhaltungsinteressen in einer Weise verletzt werden, die einer Bloßstellung in der Öffentlichkeit gleichkommt.³⁸⁶

b) Verwendung von Daten nur nach Treu und Glauben (§ 6 Abs 1 Z 1 DSGVO)

Ebenfalls in der bereits genannten Entscheidung aus dem Jahr 2005³⁸⁷ finden sich Leitlinien für die Interpretation des § 6 Abs 1 Z 1 DSGVO. § 6 DSGVO normiert Grundsätze für die Verwendung von Daten. Gem § 6 Abs 1 Z 1 dürfen Daten nur „nach Treu und Glauben und auf rechtmäßige Weise verwendet werden“³⁸⁸.

Der OGH hat entschieden, dass dieser Grundsatz eine entsprechende Benachrichtigung des Betroffenen erfordert, „um ihm die Möglichkeit zu geben, sich gegen eine seiner Meinung nach nicht gerechtfertigte, seine Kreditwürdigkeit aber massiv beeinträchtigende Datenverwendung zur Wehr zu setzen“³⁸⁹. Wenn eine Eintragung in die Warnliste entgegen diesem Grundsatz vorgenommen wird, ist sie nicht mehr durch ein überwiegendes Gläubigerschutzinteresse gerechtfertigt und somit rechtswidrig.³⁹⁰

Auch andere Entscheidungen interpretieren die Bestimmung in diese Richtung.³⁹¹ Ebenso spricht der OGH in diesem Zusammenhang aus, dass „ein <durchschnittlich informierter Betroffener> nicht damit rechnen muss, dass ein Inkassounternehmen Daten, die die Einziehung einer Forderung betreffen, zu der es gemäß § 118 Abs 3 GewO nicht berechtigt

³⁸³ OGH 17.12.2009, 6 Ob 247/08d.

³⁸⁴ OGH 17.12.2009, 6 Ob 247/08d mit Verweis auf OGH 15.12.2005, 6 Ob 275/05t.

³⁸⁵ OGH 17.12.2009, 6 Ob 247/08d.

³⁸⁶ Vgl OGH 17.12.2009, 6 Ob 247/08d.

³⁸⁷ OGH 15.12.2005, 6 Ob 275/05t.

³⁸⁸ § 6 Abs 1 Z 1 DSGVO.

³⁸⁹ *Koziol*, OGH 15.12.2005, 6 Ob 275/05t, ÖBA 2006, 530 (533).

³⁹⁰ OGH 15.12.2005, 6 Ob 275/05t.

³⁹¹ OGH 06.11.2008, 6 Ob 220/08h; OGH 12.11.2009, 6 Ob 156/09y; OGH 17.12.2009, 6 Ob 247/08d.

ist, an einen anderen iSd § 4 Z 12 DSG übermittelt, der Daten zur Auskunftserteilung über die Kreditwürdigkeit des Betroffenen in seine Datenbank aufnimmt.“³⁹²

2. OGH 19.11.2002, 4 Ob 179/02f et altera:

In mehreren Entscheidungen³⁹³ hat der OGH ausgesprochen, dass wenn ein Kunde der Offenbarung des Bankgeheimnisses ausdrücklich und schriftlich zustimmt³⁹⁴, der Kunde auch über das Widerspruchsrecht des § 28 DSG belehrt werden muss. Andernfalls widerspräche eine Klausel insoweit gegen das Transparenzgebot des § 6 Abs 3 KSchG als sie keinen Hinweis auf die Möglichkeit enthält, die danach erteilte Zustimmung zur Datenübermittlung später zu widerrufen. Fehlt ein Hinweis auf das Widerspruchsrecht des § 28 DSG, wirkt sich dies nach der Judikatur des OGH jedoch nicht auf die Zulässigkeit der Klausel aus.³⁹⁵

Im konkreten Sachverhalt stimmte der Kunde in einer Klausel der AGB³⁹⁶ der Übermittlung folgender Daten an die Kleinkreditevidenz und die Warnliste sowie an Refinanzierungsgeber des Kreditinstituts, denen gegenüber die Forderungen des Kreditinstituts gegen den Kunden als Sicherheit dienen sollen (insbesondere Österreichische Nationalbank, Österreichische Kontrollbank AG, Europäische Zentralbank, Europäische Investitionsbank) zu und entband in diesen Fällen das Kreditinstitut ausdrücklich auch vom Bankgeheimnis:³⁹⁷ Name, Anschrift, Geburtsdatum, Höhe der Verbindlichkeit, Rückführungsmodalitäten, Schritte des Kreditinstituts im Zusammenhang mit der Fälligkeitstellung und der Rechtsverfolgung sowie den Missbrauch von Zahlungsverkehrsinstrumenten.

Auch in anderen Entscheidungen sprach der OGH aus, dass die Nichterwähnung der Widerrufsmöglichkeit dem Kreditnehmer ein unklares Bild seiner vertraglichen Position vermittelt und dazu führen kann, dass er in Unkenntnis seiner Rechte an ihrer Ausübung gehindert wird, zumal eine Kenntnis der Widerrufsmöglichkeit nicht vorausgesetzt werden kann.³⁹⁸

³⁹² OGH 17.12.2009 6 Ob 247/08d.

³⁹³ Erstmals in OGH 19.11.2002, 4 Ob 179/02f.

³⁹⁴ Vgl § 38 Abs 2 Z 5 BWG.

³⁹⁵ *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (147).

³⁹⁶ Z 26 der Allgemeinen Geschäftsbedingungen für Banken idF September 2000.

³⁹⁷ *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (146).

³⁹⁸ OGH 20.03.2007, 4 Ob 221/06p und OGH 12.10.2011, 7 Ob 68/11t; ähnlich zur Pflicht zum Hinweis auf bestimmte Rechtsfolgen bei OGH 22.02.2006, 9 Ob 12/06i – dort mit Verweis auf OGH 22.03.2001, 4 Ob 28/01y und OGH 13.09.2001, 6 Ob 16/01y.

Im Exkurs „Bank AGB 2000 – mehrere Klauseln unwirksam“³⁹⁹ werde ich noch ausführlicher auf die Entscheidung OGH 19.11.2002, 4 Ob 179/02f eingehen. Es sei lediglich erwähnt, dass *Rummel* in seiner Glosse zu OGH 20.03.2007, 4 Ob 221/06p anmerkt, dass diese Entscheidung in einer mittlerweile schon recht langen Reihe von Fällen stehe, „in denen der OGH auf breiter Front und in verschiedenen Branchen AGB-Klauseln für ungültig erklärt, deren Verwendung jahrzehntelang niemand problematisiert hatte.“⁴⁰⁰

3. OGH 22.03.2001, 4 Ob 28/01y et altera:

In diesem Verfahren beanstandete der Verein für Konsumenteninformation (VKI) als Kläger Bestimmungen, welche die beklagte Bank in ihren „Besonderen Bedingungen für die Führung von Privatkonten und die Abholung von Kontopost“⁴⁰¹ verwendet. Der VKI beehrte, die beklagte Bank schuldig zu erkennen, im geschäftlichen Verkehr mit Verbrauchern in Allgemeinen Geschäftsbedingungen, die sie von ihr geschlossenen Verträgen zugrunde legt und/oder in hierbei verwendeten Vertragsformblättern die Verwendung von sechs angeführten Klauseln oder die Verwendung sinngleicher Klauseln zu unterlassen, sowie sich in bereits geschlossenen Verträgen auf diese Klauseln zu berufen und das Urteil zu veröffentlichen.

Eine Klausel davon lautete:

„Der Kontoinhaber ist damit einverstanden, dass die Bank alle im Zusammenhang mit der Eröffnung und Führung des Kontos/Depots stehenden Daten an eine zentrale Evidenzstelle und/oder an Gemeinschaftseinrichtungen von Kreditunternehmen übermitteln kann.“

Es wurde geprüft, ob ein Verstoß gegen das Transparenzgebot des § 6 Abs 3 KSchG vorliegt. Die Bestimmung wurde vom OGH als intransparent angesehen, weil sie die Tragweite der Einwilligung nicht erkennen lässt.⁴⁰² Auch kann eine wirksame Zustimmung nur dann vorliegen, wenn der Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden sollen.⁴⁰³

³⁹⁹ Vgl IV.F Exkurs: Bank AGB 2000 – mehrere Klauseln unwirksam.

⁴⁰⁰ *Rummel* in *Koziol*, OGH 20.03.2007, 4 Ob 221/06p, ÖBA 2007, 981 (996).

⁴⁰¹ Fassung April 1999.

⁴⁰² OGH 22.03.2001, 4 Ob 28/01y (= SZ 74/52) und OGH 15.12.2005, 6 Ob 275/05t.

⁴⁰³ Vgl auch OGH 22.04.2010, 2 Ob 1/09z.

In anderen Entscheidungen wurde festgehalten, dass das Transparenzgebot nicht bloß formale Verständlichkeit im Sinn von Lesbarkeit verlangt, sondern auch Sinnverständlichkeit.⁴⁰⁴ Diese kann etwa fehlen, wenn „zusammenhängende Regelungen und ihre nachteiligen Effekte deshalb nicht erkennbar werden, weil die einzelnen Teile an versteckten oder nur schwer miteinander in Zusammenhang zu bringenden Stellen, etwa in verschiedenen Klauseln, geregelt sind.“⁴⁰⁵

Durch das Transparenzgebot soll eine durchschaubare, möglichst klare und verständliche Formulierung allgemeiner Geschäftsbedingungen sichergestellt werden, damit der für die jeweilige Vertragsart typische Verbraucher seine Rechte durchsetzen kann und ihm keine unberechtigten Pflichten abverlangt werden.⁴⁰⁶

Zum Bereich Transparenzgebot und Bestimmungen in Allgemeinen Geschäftsbedingungen im Finanzdienstleistungsbereich existiert eine sehr umfangreiche Rechtsprechung. Ergänzend verweise ich an dieser Stelle nochmals auf den Exkurs „Bank AGB 2000 – mehrere Klauseln unwirksam“, in dem ich eine konkrete Klauselentscheidung ausführlich schildere.

„Das Transparenzgebot soll eine durchschaubare, möglichst klare und verständliche Formulierung allgemeiner Geschäftsbedingungen sicherstellen, um zu verhindern, dass der für die jeweilige Vertragsart typische Verbraucher von der Durchsetzung seiner Rechte abgehalten wird oder ihm unberechtigt Pflichten abverlangt werden. Das setzt die Verwendung von Begriffen voraus, deren Bedeutung dem typischen Verbraucher geläufig sind oder von ihm jedenfalls festgestellt werden können. Das können naturgemäß auch Fachbegriffe sein, nicht aber Begriffe, die so unbestimmt sind, dass sich ihr Inhalt jeder eindeutigen Festlegung entzieht. Der durch ihre Verwendung geschaffene weite Beurteilungsspielraum schließt es aus, dass der Verbraucher Klarheit über seine Rechte und Pflichten gewinnen kann.“⁴⁰⁷

⁴⁰⁴ OGH 13.09.2001, 6 Ob 16/01y und OGH 04.05.2006, 9 Ob 15/05d; ähnlich: OGH 05.06.2007, 10 Ob 67/06k; OGH 17.03.2010, 7 Ob 13/10b; OGH 27.05.2010, 5 Ob 64/10p; OGH 22.10.2010, 7 Ob 109/09v.

⁴⁰⁵ OGH 13.09.2001, 6 Ob 16/01y mit Verweis auf *Korinek*, JBl 1999, 149 (153) und *Wolf* in *Wolf/Horn/Lindacher*, AGB Gesetz⁴ § 9 Rz 148.

⁴⁰⁶ OGH 17.01.2007, 7 Ob 131/06z (= SZ 2007/2); OGH 17.01.2007, 7 Ob 140/06y; OGH 17.01.2007, 7 Ob 173/06a; OGH 02.04.2009, 8 Ob 119/08w; OGH 13.05.2009, 7 Ob 230/08m; OGH 23.11.2010, 1 Ob 164/10i; OGH 11.05.2011, 7 Ob 173/10g; OGH 07.06.2011 5 Ob 42/11d et altera.

⁴⁰⁷ OGH 11.08.2005, 4 Ob 88/05b mit Verweis auf OGH 22.03.2001, 4 Ob 28/01y und OGH 13.09.2001, 6 Ob 16 /01y; ähnlich: OGH 07.11.2007, 6 Ob 110/07f (zum Begriff der „Retrozession“ im Zusammenhang mit einem Vermögensverwaltungsvertrag); OGH 11.03.2008, 4 Ob 5/08a; OGH 28.01.2009, 10 Ob 70/07b; OGH 16.04.2009, 2 Ob 137/08y; OGH 17.03.2010, 7 Ob 15/10x;

Es wird der Durchschnittskunde als Maßstab angenommen.⁴⁰⁸

Mit aktuellem Stand⁴⁰⁹ wurden vom OGH rund 40 Fälle im Zusammenhang mit dem Datenschutzgesetz entschieden und daraus etwa 80 Rechtssätze gebildet, wobei die ältesten Judikate bis ins Jahr 1983 reichen.

5. Vergleichbare Systeme in Deutschland

In Deutschland hat „SCHUFA“ als Schutzgemeinschaft für allgemeine Kreditsicherung die Aufgabe, Informationen über Kreditabwicklungen zu sammeln und Auskünfte darüber zu geben, um dadurch das Geschäftsrisiko ua von Kreditinstituten zu minimieren.⁴¹⁰ Bei der Eröffnung eines Guthabenkontos liegt ein solches Geschäftsrisiko und damit auch ein berechtigtes Interesse der Kreditinstitute an einer entsprechenden Datenübermittlung nicht vor.⁴¹¹ Eine Einwilligung des Betroffenen ermöglicht – wie in Österreich – die datenschutzrechtliche Zulässigkeit einer Datenverwendung, wobei diese freiwillig zu erfolgen hat. Um am wirtschaftlichen Leben teilnehmen zu können, ist mittlerweile ein Girokonto unverzichtbar. Ähnliche „SCHUFA-Klauseln“ finden sich bei allen deutschen Kreditinstituten. „Die Einwilligung in eine Schufaanfrage ist daher unter dem wirtschaftlichen Druck zum Führen eines Girokontos kaum als freiwillig zu bewerten.“⁴¹² Durch die SCHUFA-Klausel wird auch die erforderliche Befreiung des Kreditinstituts vom Bankgeheimnis erklärt.⁴¹³

Die Vereinbarung, dass eine Bank berechtigt ist, eine SCHUFA-Auskunft einzuholen, begründet nach anderen Autoren keinen Sittenverstoß.⁴¹⁴

2010 verfügte SCHUFA mit ihren rund 6.000 Vertragspartnern über 479 Millionen Informationen von über 66,2 Millionen natürlichen Personen.⁴¹⁵ Dass sich der Umfang der zu speichernden Daten aus der SCHUFA-Klausel ergibt und nicht gesetzlich normiert ist, ist durchaus bemerkenswert. Angesichts des angesprochenen wirtschaftlichen Drucks auf den

⁴⁰⁸ OGH 27.03.2007, 1 Ob 241/06g; ähnlich: OGH 19.05.2009, 3 Ob 12/09z; OGH 18.09.2009, 6 Ob 128/09f; zur Anwendung auf einen Unternehmer vgl *Apathy*, Auswirkungen der Judikatur zu Verbraucherverträgen auf Bankgeschäfte mit Unternehmern, ÖBA 2004, 737 (741).

⁴⁰⁹ Stand: August 2013.

⁴¹⁰ *Rudolf/Kötterheinrich* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 5, Rz 5, S 143.

⁴¹¹ Vgl *Rudolf/Kötterheinrich* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 5, Rz 5, S 143.

⁴¹² *Rudolf/Kötterheinrich* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 5, Rz 5 letzter Satz, S 143.

⁴¹³ *Beckhusen* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 6, Rz 57, S 175.

⁴¹⁴ Für alle: *Artz* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 32, Rz 22, S 1021.

⁴¹⁵ Jahresbericht 2010 von SCHUFA, Seite 22 -
http://www.schufa.de/media/teamwebservices/unternehmen/downloads/Schufa_JB_2010_de.pdf (Stand: 18.08.2013).

einzelnen Kunden, ist dieses System vor allem betreffend qualitative Erweiterungen der bestehenden Daten zu hinterfragen. Das derzeitige System wird jedoch mit Verweis auf die – in Österreich ebenso erforderliche – notwendige Bestimmtheit der SCHUFA-Klausel als zulässig erachtet.

D. Kleinkreditevidenz

1. Begriff

Auch die sog. Kleinkreditevidenz ist als Informationsverbundsystem iSd § 50 DSG geführt. Laut Bescheid vom 12.12.2007⁴¹⁶, mit welchem dem Auftraggeber mehrere Auflagen erteilt wurden, handelt es sich hierbei um die „Kleinkreditevidenz (Konsumentenkreditevidenz) zum Zweck des Gläubigerschutzes und der Risikominimierung“. Auf die Auflagen werde ich unter „Zulässigkeit“ eingehen.

2. Beinhaltete Daten

Im der KKE dürfen folgende Daten eingetragen werden

- die Ablehnung eines Antrags auf Einräumung eines 300 Euro übersteigenden Kredits wegen mangelnder Bonität für die Dauer von 6 Monaten⁴¹⁷,
- Kredit- oder Leasingverträge über eine 300 Euro übersteigende Summe für den im Bescheid genauer umschriebenen Zeitraum⁴¹⁸.

Es werden somit folgende Daten in der KKE gespeichert:⁴¹⁹

- Personendaten (Name, Geburtsdatum, Adresse),
- Daten zu Finanzierung wie Höhe bzw Rahmen des Kredites, Gewährungsdatum, Laufzeit, Rückzahlungsdatum, Mitverpflichtete und
- Zahlungsschwierigkeiten (Mahnung, Fälligstellung etc).

3. Zulässigkeit

Informationspflichten:

Bevor ein Betroffener in die KKE eingetragen werden kann, muss ihn der Auftraggeber (zeitnah zum Abschluss bzw zur Ablehnung einer Kreditvereinbarung) darüber informieren,

- „dass einer der Gründe vorliegt, die zu einer Eintragung in die KKE führen,
- dass die KKE ein zu Zwecken des Gläubigerschutzes und der Risikominimierung geführtes Informationsverbundsystem (§ 50 DSG 2000) von Kreditinstituten,

⁴¹⁶ DSK 12.12.2007, K600.033-018/0002-DVR/2007.

⁴¹⁷ Vgl DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „1.a)“ des Spruches.

⁴¹⁸ Vgl DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „1.b)“ des Spruches.

⁴¹⁹ Vgl Informationsblatt des KSV 1870 für Privatpersonen (Stand Februar 2013), Seite 3 - http://www.ksv.at/KSV/1870/de/pdf/964Informationsblatt_Privatpersonen.pdf (Stand: 18.08.2013).

kreditgebenden Versicherungsunternehmen und Leasingunternehmen darstellt, dessen Betreiber (iSd § 50 DSG 2000) der Kreditschutzverband von 1870 (KSV) ist,

- *dass Daten aus der KKE ausschließlich an Kreditinstitute, kreditgewährende Versicherungsunternehmen und Leasinggesellschaften mit Sitz in einem Mitgliedstaat des europäischen Wirtschaftsraums (EWR) auf Anfrage weitergegeben werden, soweit diese eine Rechtspflicht zur korrekten Beurteilung des Kreditrisikos, das ein Kreditwerber darstellt, trifft,*
- *welche Rechtsbehelfe im Falle der Eintragung zur Verfügung stehen und wo sie einzubringen sind.*⁴²⁰

Wenn Daten aus der 2007 bereits bestehenden Kleinkreditevidenz des KSV übernommen werden, ist sicherzustellen, dass die Betroffenen über diese Punkte informiert werden, soweit sie nicht schon nachweislich darüber informiert wurden.

Bestreitungsvermerk:

Wenn eine begründete Bestreitung einer Kapital- oder Zinsforderung dem Grund oder der Höhe nach vorliegt, hat der Auftraggeber zu veranlassen, dass dies in der KKE unverzüglich durch einen Bestreitungsvermerk ersichtlich gemacht wird. Sofern der Schuldner es verlangt, sind auch diesbezügliche noch nicht rechtskräftige gerichtliche Entscheidungen in der KKE anzumerken.⁴²¹

Pflicht zur Richtigstellung:

Wenn die Unrichtigkeit der in der KKE ausgewiesenen Höhe eines Schuldbetrages rechtskräftig festgestellt wurde, hat der Auftraggeber die Berichtigung unverzüglich zu veranlassen.⁴²² Wenn das Nicht-Bestehen einer Schuld rechtskräftig festgestellt wurde, sind alle diesbezüglichen Eintragungen in der KKE unverzüglich zu streichen.⁴²³

Die teilnehmenden Auftraggeber (diverse Kreditinstitute, kreditgebende Versicherungsunternehmen und Leasingunternehmen sowie der KSV – Kreditschutzverband von 1870) und der Betreiber (KSV) haben alle zumutbaren Anstrengungen zu unternehmen,

⁴²⁰ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „2. a) bis d)“ des Spruches.

⁴²¹ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „4.“ des Spruches.

⁴²² DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „5.“ des Spruches, Satz 1.

⁴²³ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „5.“ des Spruches, Satz 2.

„um die eingetragenen Daten hinsichtlich ihrer Richtigkeit jeweils auf aktuellem Stand zu halten“⁴²⁴.

Insbesondere „hat der Auftraggeber dafür Vorsorge zu treffen, dass die von ihm zu verantwortenden Datensätze in der KKE, die sich auf einen Zahlungsanstand beziehen, mindestens einmal jährlich, alle anderen Datensätze spätestens alle drei Jahre auf ihre Richtigkeit und Aktualität überprüft werden.“⁴²⁵

Löschungsverpflichtungen:

In folgenden Fällen sind die in der KKE gespeicherten Daten zu löschen:

- Die Ablehnung eines Antrags auf Einräumung eines 300 Euro übersteigenden Kredits wegen mangelnder Bonität: nach sechs Monaten.⁴²⁶
- Wenn rechtskräftig festgestellt wurde, dass eine Schuld nicht besteht, müssen alle diesbezüglichen Eintragungen unverzüglich aus der KKE gestrichen werden.⁴²⁷
- „Wenn eine Kredit- oder Leasingschuld ohne Zahlungsanstand vollständig abbezahlt und das Kredit- oder Leasingverhältnis somit beendet ist: spätestens 90 Tage nach Abbezahlung.“⁴²⁸
- „Wenn das Nichtbestehen des behaupteten Zahlungsanstandes rechtskräftig festgestellt wurde: spätestens 90 Tage nach vollständiger Abbezahlung der Schuld bzw wenn die Feststellung erst nach dieser Frist erfolgte: unverzüglich nach rechtskräftiger Feststellung.“⁴²⁹
- „Wenn eine Kredit- oder Leasingschuld nach Zahlungsanstand vollständig abbezahlt wurde: spätestens fünf Jahre nach vollständiger Abzahlung der Schuld.“⁴³⁰
- „In allen anderen Fällen: sieben Jahre nach Tilgung der Schuld oder Eintritt eines sonstigen schuldbefreienden Ereignisses.“⁴³¹

In der KKE werden im Unterschied zur „Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf

⁴²⁴ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „9.“ des Spruches, Satz 1.

⁴²⁵ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „9.“ des Spruches, Satz 2.

⁴²⁶ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „1. a)“ des Spruches.

⁴²⁷ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „5.“ des Spruches, Satz 2.

⁴²⁸ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „6. a)“ des Spruches.

⁴²⁹ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „6. c)“ des Spruches.

⁴³⁰ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „6. b)“ des Spruches.

⁴³¹ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „6. d)“ des Spruches.

vertragswidriges Kundenverhalten“ auch Positivdaten gespeichert. Es handelt sich hierbei um Daten über Kreditverhältnisse ohne Zahlungsanstand.⁴³²

Es können daher auch Daten gespeichert werden, ohne dass Zahlungsanstand vorliegt. Es muss also kein vertragswidriges Verhalten zur Aufnahme in die KKE vorliegen. Die Informationspflichten der Auftraggeber gegenüber dem Betroffenen sind aber jedenfalls zu beachten.

Diverse Rechte und Pflichten laut DSGVO:

Beim Betreiber (KSV) ist nach den erteilten Auflagen der DSK eine „Auskunfts- und Beschwerdestelle für alle Anbringen der in die KKE Eingetragenen einzurichten, die auch Auskunftsbegehren nach § 26 DSGVO und Richtigstellungs- und Löschungsbegehren nach § 27 DSGVO entgegennimmt und für deren Bearbeitung durch den Auftraggeber sorgt.“⁴³³

Wenn ein Löschungsbegehren nach § 27 DSGVO abgelehnt wird, wird dadurch das Widerspruchsrecht des Betroffenen nach § 28 Abs 1 DSGVO nicht berührt.⁴³⁴ Dies soll die Bedeutung des Widerspruchsrechts als das Mittel der Wahl zur Erreichung einer adäquaten Lösung klarstellen. Die seit der Registrierung der „Warnliste der Banken“ gewonnenen praktischen Erfahrungen wurden somit eingearbeitet.⁴³⁵

Verhältnis der Warnliste und der KKE zum VKrG:

§ 7 VKrG⁴³⁶ schreibt vor, dass der Kreditgeber vor Abschluss des Kreditvertrags die Kreditwürdigkeit des Verbrauchers anhand ausreichender Informationen zu prüfen hat, „die er – soweit erforderlich – vom Verbraucher verlangt“⁴³⁷. Der Kreditgeber hat erforderlichenfalls auch Auskünfte aus einer zur Verfügung stehenden Datenbank einzuholen. Grundlage der österr Bestimmung ist die Verbraucherkreditrichtlinie⁴³⁸. Die RL wollte damit nicht die Schaffung einer Datenbank verlangen, sondern an den vorhandenen faktischen und

⁴³² Vgl. Reimer in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 568 mit Verweis auf den Registrierungsbescheid DSK 12.12.2007, K600.033-018/0002-DVR/2007.

⁴³³ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „7.“ des Spruches.

⁴³⁴ DSK 12.12.2007, K600.033-018/0002-DVR/2007, Punkt „8.“ des Spruches.

⁴³⁵ Vgl. DSK 12.12.2007, K600.033-018/0002-DVR/2007, „Rechtliche Erwägungen“.

⁴³⁶ BGBl I Nr 28/2010: Bundesgesetz über Verbraucherkreditverträge und andere Formen der Kreditierung zu Gunsten von Verbrauchern (Verbraucherkreditgesetz – VKrG).

⁴³⁷ § 7 Abs 1 VKrG.

⁴³⁸ Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (= ABl L 133 vom 22.05.2008, S 66–92).

rechtlichen Status quo im jeweiligen Mitgliedstaat anknüpfen.⁴³⁹ In Österreich kommen va die Warnliste⁴⁴⁰ und die KKE in Betracht.⁴⁴¹

Eine besondere Bestimmung wurde im Zuge des Gesetzgebungsverfahrens sehr spät in § 7 Abs 5 VKrG eingefügt: Demnach ist § 28 Abs 2 DSG auf bei der DSK registrierte Informationsverbundsysteme kreditgebender Institutionen zur Bonitätsbeurteilung, bei denen die Verwendung auf § 8 Abs 1 Z 2 oder Z 4 DSG beruht, nicht anzuwenden. Damit soll etwa die Einordnung der Warnliste oder der KKE als öffentliche Datenbank iSd § 28 Abs 2 DSG verhindert werden und somit kein Widerspruchsrecht gem § 28 Abs 2 DSG bestehen.⁴⁴²

Auch wenn eine Bonitätsprüfung negativ verläuft, kann der Kreditgeber den Kreditvertrag mit dem Verbraucher trotzdem abschließen, „sofern er den Verbraucher über diesen Umstand nur ausreichend informiert hat.“⁴⁴³ Durch § 7 VKrG soll nach *Zöchling-Jud* sowohl das Interesse an einer funktionstüchtigen Kreditwirtschaft, als auch der individuelle Kreditnehmer vor einem über seine finanziellen Verhältnisse abgeschlossenen Kreditvertrag geschützt werden.⁴⁴⁴

Zu den zivilrechtlichen Rechtsfolgen bei Verstößen gegen § 7 VKrG gibt es bereits umfangreiche Literatur.⁴⁴⁵ Über die konkrete Höhe des Schadens, der dem Verbraucher als Folge einer nicht erfolgten oder mangelhaften Prüfung seiner Kreditwürdigkeit, oder auch einer nicht erfolgten Warnung, entstehen kann, herrscht Uneinigkeit im Schrifttum.⁴⁴⁶ Manche befürworten als Alternative den „aufsichtsrechtlichen Weg“, der jedoch Branchen außerhalb der Kreditwirtschaft im derzeitigen Regelungsregime nicht erfassen würde.⁴⁴⁷ Klarstellende Rsp zur Höhe des ersatzfähigen Schadens⁴⁴⁸ oder auch eine genaue Normierung

⁴³⁹ *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 21.

⁴⁴⁰ Vgl IV.C Warnliste der österreichischen Kreditinstitute.

⁴⁴¹ *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 22.

⁴⁴² Vgl näher *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 24 f mit Verweis auf den Abänderungsantrag 117 Blg NR 24. GP, 9.

⁴⁴³ *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 32.

⁴⁴⁴ *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 1.

⁴⁴⁵ Vgl *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 41 ff sowie *Leupold/Ramharter*, Die Verletzung der Pflicht zur Warnung vor mangelnder Kreditwürdigkeit nach dem Verbraucher kreditgesetz – Europarechtliche Grundlagen und zivilrechtliche Konsequenzen, ÖBA 2011, 469 (476 ff) und *Weissel*, Zur Anwendung von § 7 VKrG, ÖBA 2012, 302 (307 ff), jeweils mwN.

⁴⁴⁶ *Weissel*, Zur Anwendung von § 7 VKrG, ÖBA 2012, 302 (309).

⁴⁴⁷ *Weissel*, Zur Anwendung von § 7 VKrG, ÖBA 2012, 302 (310).

⁴⁴⁸ *Zöchling-Jud* in *Wendehorst/Zöchling-Jud*, Verbraucher kreditrecht (2010), § 7 Rz 45 f sowie *Leupold/Ramharter*, Die Verletzung der Pflicht zur Warnung vor mangelnder Kreditwürdigkeit nach dem Verbraucher kreditgesetz – Europarechtliche Grundlagen und zivilrechtliche Konsequenzen, ÖBA 2011, 469 (479 ff).

der zivilrechtlichen Folgen einer vom Kreditgeber zu verantwortenden Missachtung von § 7 VKrG⁴⁴⁹ bleiben daher abzuwarten.

§ 8 VKrG ermöglicht bei grenzüberschreitenden Krediten im Bereich der Vertragsstaaten des EWR den Zugang zu Datenbanken, die zur Bewertung der Kreditwürdigkeit des Verbrauchers verwendet werden.⁴⁵⁰

ME ist es zu begrüßen, dass die Warnliste und die KKE im VKrG erstmals gesetzlich erwähnt werden, wenn sie auch nicht explizit benannt werden. Durch die Regelung in § 7 Abs 1 VKrG wird die Pflicht zur Bonitätsprüfung, erforderlichenfalls die Abfrage einer zur Verfügung stehenden Datenbank, normiert. Die Zulässigkeit der beiden Datenbanken beruht aber auf den beiden Musterbescheiden der DSK.

Im Anschluss an *Kotschy* fehlen somit nach wie vor Regelungen über die Rahmenbedingungen für die Führung der Bonitätsdatenbanken selbst.⁴⁵¹ Da detaillierte gesetzliche Regelungen, „die einen Ausgleich zwischen den Informationsinteressen der Kreditgeber einerseits und den Datenschutzinteressen der Kreditwerber andererseits herstellen“⁴⁵², fehlen, gibt es nach *Kotschy* weder verlässliche Kreditinformation noch verlässlichen Datenschutz für jedermann.⁴⁵³

Dieser Meinung kann ich mich nur anschließen. Auch das deutsche Bundesdatenschutzgesetz enthält seit dem BGBl 2009 I, S 2254⁴⁵⁴ „einheitliche Voraussetzungen für die Übermittlung von Daten über Forderungen an Auskunftteien, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist“⁴⁵⁵. Folglich gibt es selbst in einem für das Funktionieren der Wirtschaft so grundlegenden Bereich wie den Bonitätsdatenbanken in Österreich kaum gesetzliche Regelungen für deren Betrieb. Die von *Kotschy* als ehemaliges geschäftsführendes Mitglied der DSK vorgeschlagenen Bereiche⁴⁵⁶ sind dabei zu berücksichtigen, wenngleich im

⁴⁴⁹ *Weissel*, Zur Anwendung von § 7 VKrG, ÖBA 2012, 302 (309 f) mwN.

⁴⁵⁰ Vgl § 8 1. Satz VKrG.

⁴⁵¹ *Kotschy*, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 307 (310).

⁴⁵² *Kotschy*, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 307 (310).

⁴⁵³ Weitere Einzelheiten und erforderliche gesetzliche Rahmenbedingungen: *Kotschy*, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 307 (310 ff).

⁴⁵⁴ Gesetz zur Änderung des Bundesdatenschutzgesetzes (Deutsches BGBl 2009 I, Nr 48, S 2254).

⁴⁵⁵ *Pauly/Ritzer*, Datenschutz-Novellen: Herausforderungen für die Finanzbranche, WM 2010, 8 (10); Zu den deutschen Normen in § 28a Abs 1 BDSG im Detail: *Pauly/Ritzer*, Datenschutz-Novellen: Herausforderungen für die Finanzbranche, WM 2010, 8 (10 f).

⁴⁵⁶ Wer darf Bonitätsdatenbanken führen?; Welche Daten sollen verarbeitet werden dürfen?; Aus welchen Quellen dürfen bonitätsrelevante Daten ermittelt werden?; Wann sind Daten zu löschen?; Wem darf Zugang zu

Sinne der Überschaubarkeit und Vermeidung einer Zersplitterung gesetzlicher Regelungen einzelne Bereiche in allgemeinen Bereichen des Datenschutzgesetzes bzw in der derzeit diskutierten Datenschutz-VO⁴⁵⁷ eingebaut werden könnten, zB das Lösungsrecht des Betroffenen und der Grundsatz der Datenrichtigkeit.

4. Judikatur der österr DSK

Auch im Bereich der KKE erstreckt sich die Judikatur im Wesentlichen auf Entscheidungen über Auskunftsbegehren.⁴⁵⁸

Des Weiteren findet sich ein Genehmigungsbescheid zum Informationsverbundsystem KKE in der Judikatur der DSK.⁴⁵⁹ Hierbei handelt es sich um eine Mustererledigung. Damit wurde zum Ausdruck gebracht, dass gleichlautende Auflagen mit höchster Wahrscheinlichkeit allen Auftraggebern erteilt werden, die eine Teilnahme am gegenständlichen Informationsverbundsystem KKE melden.

5. Vergleichbare Systeme in Deutschland

Auch im Bereich der Kleinkredite ist in Deutschland SCHUFA von besonderer Bedeutung, weshalb ich erneut darauf verweise.⁴⁶⁰ Eine betragliche Mindestgrenze, ab der SCHUFA Kreditdaten speichern darf, findet sich in Deutschland nach dem derzeitigen Wissenstand nicht. In Österreich können bei der Kleinkreditevidenz erst Kreditverträge oder abgelehnte Kreditanträge ab EUR 300,00 eingetragen werden.⁴⁶¹

In der KKE ist die Ablehnung auf Einräumung eines EUR 300,00 übersteigenden Kredites nach sechs Monaten zu löschen. Wenn eine Kredit- oder Leasingsschuld ohne Zahlungsanstand vollständig abbezahlt wurde, ist die Eintragung spätestens 90 Tage nach Abbezahlung zu löschen. Sofern ein Zahlungsanstand vorliegt, hat die Löschung spätestens fünf Jahre nach Abbezahlung der Schuld zu erfolgen.

den Daten einer Bonitätsdatenbank eingeräumt werden?; Verbesserung der Wahrnehmung der Betroffenenrechte, der Richtigkeit von Bonitätsdaten sowie des Auskunftsrechtes.

⁴⁵⁷ Vgl V.E Reform des „europäischen Datenschutzrechtes“.

⁴⁵⁸ So etwa die stattgebende Entscheidung DSK 03.12.2002, K120.804/016-DSK/2002 und folgende abweisende Entscheidungen mangels Verletzungen des Auskunftsrechtes: DSK 07.12.2004, K120.938/0003-DSK/2004 und DSK 19.06.2009, K121.494/0013-DSK/2009.

⁴⁵⁹ DSK 12.12.2007, K600.033-018/0002-DVR/2007.

⁴⁶⁰ Vgl IV.C.5 Vergleichbare Systeme in Deutschland.

⁴⁶¹ Vgl auch Reimer in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009), 568.

In Deutschland besteht eine inhaltlich weiter reichende Möglichkeit: Es kann unter bestimmten Voraussetzungen ein kurzfristiger Zahlungsausgleich⁴⁶² vorliegen, der eine vorzeitige Löschung aus dem SCHUFA-Datenbestand zur Folge hat.

Zur vorzeitigen Löschung müssen folgende Voraussetzungen kumulativ vorliegen:⁴⁶³

- der Betrag der verspätet beglichenen Forderung ist geringer oder gleich EUR 2.000,00,
- die Forderung wurde innerhalb von sechs Wochen beglichen und vom Gläubiger der SCHUFA als beglichen gemeldet, und
- die Forderung darf nicht tituliert sein.⁴⁶⁴

Sofern eine der genannten Voraussetzungen nicht zutrifft, bleibt die bereits – jedoch mit Verspätung – bezahlte Forderung als „erledigt“ bis zum Ende der Speicherfrist (in der Regel drei Jahre) im SCHUFA-Datenbestand gespeichert.

Meines Erachtens wäre eine mit Österreich vergleichbare „Bagatellgrenze“ von zumindest EUR 300,00 bei Kleinkrediten notwendig, um zu vermeiden, dass auch Daten zu Kreditverträgen über Kleinstbeträge von SCHUFA gespeichert werden.

In Art 9 der Verbraucherkreditrichtlinie⁴⁶⁵ ist eine Art „Minidatenschutzrecht“ enthalten⁴⁶⁶. Demnach stellt bei grenzüberschreitenden Krediten jeder Mitgliedstaat sicher, dass Kreditgeber aus anderen Mitgliedstaaten Zugang zu den in seinem Hoheitsgebiet zur Bewertung der Kreditwürdigkeit des Verbrauchers verwendeten Datenbanken haben, wobei dieser Zugang ohne Diskriminierung zu gewähren ist.⁴⁶⁷

⁴⁶² Darunter wird eine innerhalb eines Monats beglichene Forderung verstanden, bei der bereits ein Zahlungsanstand vorliegt.

⁴⁶³ Diese sowie weitere Informationen zur SCHUFA finden sich auf deren Webseite: http://www.schufa.de/de/private/wissenswertes/gespeicherteinformationen/loeschen_von_informationen/loeschen_von_informationen.jsp (Stand: 18.08.2013).

⁴⁶⁴ ZB darf ein Vollstreckungsbescheid iSd deutschen Gesetzes nicht vorliegen. Nach der österr Terminologie dürfte wohl kein Exekutionstitel bestehen. Auf die Frage, inwiefern der Vollstreckungsbescheid mit dem bedingten Zahlungsbefehl vergleichbar ist, werde ich in dieser Dissertation nicht eingehen, da hierfür ein ausführlicherer zivilverfahrensrechtlicher Vergleich notwendig wäre, was den Umfang dieser Arbeit wohl übersteigen würde.

⁴⁶⁵ Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (= ABl L 133 vom 22.05.2008, S 66–92).

⁴⁶⁶ Vgl Reimer in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009), 569.

⁴⁶⁷ Vgl Art 9 Abs 1 der RL 2008/48/EG.

Wenn ein Kreditantrag aufgrund einer Datenbankabfrage abgelehnt wird, so hat der Kreditgeber den Verbraucher unverzüglich und unentgeltlich über das Ergebnis dieser Abfrage und über die Angaben der betreffenden Datenbank zu informieren.⁴⁶⁸

Art 9 Abs 4 der RL 2008/48/EG normiert, dass Art 9 der RL 2008/48/EG unbeschadet der Datenschutzrichtlinie⁴⁶⁹ gilt. Somit enthält Art 9 der RL 2008/48/EG im Vergleich zur RL 1995/46/EG speziellere Bestimmungen zum Datenschutzrecht im Bereich der Verbraucherkredite. In Art 9 nicht geregelte datenschutzrechtliche Fragen sind aber nach wie vor nach der RL 1995/46/EG bzw den innerstaatlichen Bestimmungen, die in Umsetzung der RL 1995/46/EG ergangen sind, zu lösen.

⁴⁶⁸ Vgl Art 9 Abs 2 der RL 2008/48/EG.

⁴⁶⁹ RL 1995/46/EG.

E. Mobilfunkverträge und Bonitätsdatenbanken

1. Begriff

Von besonderer Bedeutung im Geschäftsleben sind Wirtschaftsauskunftsdienste zur Auskunft über die Kreditwürdigkeit. Hierbei werden meist vor Vertragsabschluss aus bisherigem Verhalten von Privatpersonen, wie etwa Zahlungsanstände oder betriebene Exekutionsverfahren, Schlüsse für die künftige Solvenz dieser Personen gezogen. „Bonitätsauskunftsunternehmen führen Datenbanken über das Zahlungsverhalten und die Zahlungsmoral von einer Vielzahl in Österreich lebender Personen.“⁴⁷⁰ „Eine von Wirtschaftsauskunftsdiensten festgestellte mangelhafte Bonität hat für die meisten Menschen einen dramatischen Ausschluss von wirtschaftlicher Beteiligung zur Folge. (...) Ein funktionierendes System zur Beurteilung der Kreditwürdigkeit, aber auch ein(e) starke Absicherung gegen die Verbreitung falscher oder irreführender Daten sind daher wesentliche Voraussetzung für eine moderne wirtschaftliche Zusammenarbeit.“⁴⁷¹

Auf ein jüngst ergangenes Judikat⁴⁷² werde ich in diesem Kapitel besonders eingehen, da es endgültig Klarheit in vielerlei Hinsicht gebracht hat. Zuerst werde ich die für diesen Bereich zentrale Bestimmung des § 152 GewO⁴⁷³ darlegen, auf die sich viele Wirtschaftsauskunftsdienste – zu Unrecht – als gesetzliche Anordnung iSd § 28 Abs 2 DSGVO⁴⁷⁴ berufen haben:

§ 152 (1) Gewerbetreibende, die zur Ausübung des Gewerbes der Auskunfteien über Kreditverhältnisse berechtigt sind, sind nicht zur Erteilung von Auskünften über private Verhältnisse, die mit der Kreditwürdigkeit in keinem Zusammenhang stehen, berechtigt.

(2) Die im Abs 1 genannten Gewerbetreibenden sind verpflichtet, ihren geschäftlichen Schriftwechsel und die Geschäftsbücher durch sieben Jahre aufzubewahren. Die Frist von sieben Jahren läuft vom Schluss des Kalenderjahres, in dem der Schriftwechsel erfolgte oder die letzte Eintragung in das Geschäftsbuch vorgenommen wurde. Im

⁴⁷⁰ Dörfler/Siegwart in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 525.

⁴⁷¹ Krenn/Zeger in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 535.

⁴⁷² OGH 01.10.2008, 6 Ob 195/08g.

⁴⁷³ BGBl Nr 194/1994, zuletzt geändert durch BGBl I Nr 125/2013: Gewerbeordnung 1994 (GewO 1994).

⁴⁷⁴ Demnach kann der Betroffene gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datenanwendung jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben, woraufhin die Daten binnen acht Wochen zu löschen sind (vgl § 28 Abs 2 DSGVO).

Fälle der Endigung der Gewerbeberechtigung sind der Schriftwechsel und die Geschäftsbücher zu vernichten, auch wenn der Zeitraum von sieben Jahren noch nicht verstrichen ist.

Soweit „nicht-sensible“ Daten von den Wirtschaftsauskunftsdiensten verwendet werden, kann als Legitimation für die Verarbeitung von Bonitätsdaten nur auf die allgemeine Bestimmung des § 8 Abs 1 Z 4 DSGVO abgestellt werden, nach der schutzwürdige Interessen des Betroffenen dann nicht verletzt sind, wenn überwiegende berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.⁴⁷⁵ Auch die DSK ging von einer grundsätzlichen Zulässigkeit der Verarbeitung von Bonitätsdaten aus.⁴⁷⁶ Dies wird vor allem damit begründet, dass der Gesetzgeber durch die Schaffung des § 152 GewO von einer grundsätzlichen Zulässigkeit dieses Gewerbes ausgegangen ist und dass § 1052 ABGB einen Verlust des Rechts auf Sicherstellung des zur Vorausleistung verpflichteten Vertragspartners normiert, sofern diesem die schlechten Vermögensverhältnisse des anderen Teiles zur Zeit des Vertragsabschlusses nicht bekannt sein mussten.⁴⁷⁷

2. Beinhaltete Daten

Ein „überwiegendes berechtigtes Interesse“ an der Verwendung von Zahlungserfahrungsdaten sollte nur dann angenommen werden, „wenn es sich tatsächlich um einen Fall von Zahlungsunfähigkeit oder -unwilligkeit des Betroffenen handelt und nicht um eine Fallkonstellation, in der überhaupt das Bestehen einer Forderung durch den Schuldner bestritten wird.“⁴⁷⁸

Es können daher Daten über die Vermögensverhältnisse einschließlich Zahlungsunfähigkeit bzw -willigkeit eines Betroffenen verarbeitet werden.

Nicht gespeichert werden dürfen sensible Daten.⁴⁷⁹ Auch dürfen Daten über „private Verhältnisse“, die mit der Kreditwürdigkeit in keinem Zusammenhang stehen, nicht verarbeitet werden.⁴⁸⁰

⁴⁷⁵ Vgl Krenn/Zeger in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 535.

⁴⁷⁶ DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁷⁷ Krenn/Zeger in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 535 f.

⁴⁷⁸ Krenn/Zeger in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 536 f.

⁴⁷⁹ Es liegt keiner der Gründe des § 9 Z 1 bis 13 DSGVO vor, nach denen schutzwürdige Geheimhaltungsinteressen bei der Verwendung sensibler Daten nicht verletzt werden würden.

⁴⁸⁰ Vgl § 152 Abs 1 GewO.

3. Zulässigkeit

Die DSK hat gemäß § 30 Abs 6 DSG in einem Verfahren im Jahr 2007⁴⁸¹ mehrere Empfehlungen an eine Inkasso GmbH ausgesprochen.⁴⁸² Aus diesen Empfehlungen und den daraus abgeleiteten Rechtssätzen leite ich folgende Kriterien ab, die bei der Weitergabe von Inkassodaten zu beachten sind:

Zulässigkeit von Auskunfteien über Kreditverhältnisse:

Wie bereits ausführlich erörtert wurde⁴⁸³, ist aus den in § 152 GewO aufgestellten Regeln für Auskunfteien über Kreditverhältnisse von der grundsätzlichen Zulässigkeit dieser gewerblichen Tätigkeit auszugehen. Daher kann eine „rechtliche Befugnis“ iSd § 7 Abs 1 DSG vorliegen, eine gesetzliche Zuständigkeit des Auftraggebers liegt jedoch nicht vor. Die schutzwürdigen Geheimhaltungsinteressen der Betroffenen sind zu wahren.

Auch wenn in bestimmten Fallkategorien von einem überwiegendem berechtigten Interesse der Gewerbetreibenden an einer Verwendung von Daten über „Kreditverhältnisse“ auszugehen ist, sind mE auf der anderen Seite die Interessen der Betroffenen in besonderem Maße zu berücksichtigen und die Sammlung, Aufbewahrung und Weitergabe von Daten, die die Kreditwürdigkeit betreffen, nicht allgemein und uneingeschränkt zulässig.

Auch § 1052 Satz 2 ABGB lässt erkennen, dass in bestimmten Fällen von einem berechtigten Interesse der Gläubiger an der Verwendung von Bonitätsdaten auszugehen ist. Der Wunsch nach spezifischen gesetzlichen Regelungen für die Ausgestaltung von Bonitätsdatenbanken wurde auch schon geäußert.⁴⁸⁴

Die Datenanwendung, in welcher personenbezogene Daten von Inkassoschuldnern verarbeitet werden, ist beim Datenverarbeitungsregister (DVR) zu melden. Das Anführen einer DVR-Nummer eines vom Inkassoinstitut verschiedenen Auftraggebers ist nicht gestattet.⁴⁸⁵

Datenrichtigkeit:

Wenn Inkassodaten an eine Kreditauskunftei übermittelt werden, darf nur jener Forderungsbetrag als offen gemeldet werden, der im Übermittlungszeitpunkt tatsächlich noch nicht beglichen ist. Auch wenn eine Zahlung in Raten angeboten und eingehalten wird, kann

⁴⁸¹ DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁸² Vgl Empfehlungen in DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁸³ Vgl IV.E.1 Begriff.

⁴⁸⁴ *Sedef*, 1. Österreichischer IT-Rechtstag – ein Tagungsbericht, MR 2007, 241 (242 f).

⁴⁸⁵ Vgl 5. Empfehlung in DSK 07.05.2007, K211.773/0009-DSK/2007.

dies einer sofortigen Zahlung entsprechen, wenn die angebotene und eingehaltene Zahlung einer sofortigen Zahlung nahe kommt.⁴⁸⁶ Solche Ratenzahlungen dürfen nicht an eine Kreditauskunftei gemeldet werden und zählen als vertragsgemäße Erfüllung.

Informationspflichten und Schutzwürdigkeit:

Eine Weitergabe von Bonitätsdaten durch ein Inkassobüro an eine Kreditauskunftei stellt eine besondere Eingriffstiefe in das Recht auf Geheimhaltung nach § 24 Abs 2 DSG dar. Daher sind Informationen an den Betroffenen über die Voraussetzungen einer derartigen Übermittlung zu erteilen. Betroffene Schuldner sind somit bereits im ersten Mahnschreiben darüber zu informieren, ob und unter welchen Voraussetzungen ihre inkassorelevanten Daten an Kreditauskunfteien weitergegeben werden.⁴⁸⁷

Nach § 24 Abs 1 DSG hat der Auftraggeber einer Datenanwendung aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und über Namen und Adresse des Auftraggebers, zu informieren, wenn diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. Über Abs 1 leg cit hinausgehende Informationen sind zu erteilen, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist.

Bonitätsdaten kommt eine besondere Eingriffstiefe im Hinblick auf das Recht auf Geheimhaltung zu. Um das Vorliegen eines überwiegenden berechtigten Interesses an der Weitergabe von Inkassodaten an eine Kreditauskunftei zu bejahen, müssen die Aussagekraft und Richtigkeit der Daten gewährleistet sein. Da § 118 Abs 2 GewO Forderungsabtretungen zu Inkassozwecken generell verbietet, ist die Aussage, dass die Forderung eines Mandanten einem Inkassobüro abgetreten worden ist, nicht richtig und muss unterlassen werden.⁴⁸⁸ Es darf daher in einem Schreiben an betroffene Schuldner nicht behauptet werden, dass eine geltend gemachte Forderung einem Inkassounternehmen abgetreten worden sei. Inkassoinstitute⁴⁸⁹ können daher nur fremde Forderungen eintreiben.

Weiters dürfen nur die aus dem vorhergehenden Punkt⁴⁹⁰ ersichtlichen Daten verarbeitet werden.

⁴⁸⁶ Vgl 1. Empfehlung in DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁸⁷ Vgl 4. Empfehlung in DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁸⁸ Vgl 3. Empfehlung in DSK 07.05.2007, K211.773/0009-DSK/2007.

⁴⁸⁹ Vgl § 94 Z 36 GewO.

⁴⁹⁰ IV.E.2 Beinhaltete Daten.

Outsourcing von Raterstellung

In zunehmendem Ausmaß werden in den letzten Jahren in Österreich und Deutschland bankinterne Ratings über die wirtschaftliche Fähigkeit eines Kreditnehmers und seine rechtliche Bindung, den zwingend fälligen Zahlungsverpflichtungen vollständig und rechtzeitig nachzukommen, gemacht.⁴⁹¹ Schätzungen zufolge entstehen für interne Ratingverfahren Kosten in Höhe von EUR 250,00 bis 7.500,00 pro Rating, abhängig von der Datentiefe und Unternehmensgröße bei Unternehmen⁴⁹², was eine sehr große Bandbreite widerspiegelt.

Das Outsourcing setzt stets einen Informationsfluss vom Kreditinstitut bzw Auftraggeber der Bonitätsprüfung zum Dienstleister voraus.⁴⁹³ Die datenschutzrechtliche Zulässigkeit ist daher jeweils im Einzelfall zu prüfen.⁴⁹⁴

4. Judikatur der österr DSK

Die beiden folgenden Judikate schildern sehr plastisch, welche Auswirkungen ein Eintrag in Bonitätsdatenbanken haben kann und wie erfolgreich dagegen vorgegangen werden kann.

OGH 01.10.2008, 6 Ob 195/08g⁴⁹⁵:

Im vorliegenden Verfahren begehrte der Kläger die Löschung des folgenden Datensatzes:

„Letzte Änderung: 08.07.2004

Text: Exekution bewilligt

Betrag: n.b

*Gläubiger: D***** L******

*Gerichtszahl: *****.“*

Im August 2006 wollte der Kläger einen Mobilfunkvertrag mit einem Mobilfunkunternehmen abschließen, das jedoch den Vertragsabschluss verweigerte, weil in einer Bonitätsdatenbank drei den Kläger betreffende Einträge, darunter der obgenannte, aufgeschienen sind.

⁴⁹¹ Volk, Outsourcing der Raterstellung im Lichte des deutschen Datenschutzes und Bankgeheimnisses, ÖBA 2009, 372 (372).

⁴⁹² Volk, Outsourcing der Raterstellung im Lichte des deutschen Datenschutzes und Bankgeheimnisses, ÖBA 2009, 372 (373).

⁴⁹³ Vgl Schütz/Waldherr, Die Auslagerung bankgeschäftlicher Tätigkeiten aus bankaufsichtsrechtlicher Sicht (Outsourcing), ÖBA 2007, 138 (142).

⁴⁹⁴ Zu Fragen des Bankgeheimnisses sowie zum Datenschutz iZm Auslagerungen bankgeschäftlicher Tätigkeiten: Schütz/Waldherr, Die Auslagerung bankgeschäftlicher Tätigkeiten aus bankaufsichtsrechtlicher Sicht (Outsourcing), ÖBA 2007, 138 (142 f).

⁴⁹⁵ Vgl OGH 01.10.2008, 6 Ob 195/08g.

Das Erstgericht bejahte die Auftraggebereigenschaft des Betreibers der Bonitätsdatenbank.⁴⁹⁶ Gemäß „§ 28 Abs 2 DSG könne der Betroffene beim Auftraggeber gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben.“⁴⁹⁷

Für die Bonitätsdatenbank bestehe keine gesetzliche Anordnung. Auch sei sie „öffentlich zugänglich, weil sie einem nicht von vornherein bestimmten, nicht nach außen hin begrenzten Personenkreis zugänglich gemacht werde und der Zugang zur Datei nur von der Entscheidung des Auftraggebers über das „berechtigte“ Interesse des Abfragenden abhängig sei.“⁴⁹⁸

Das Berufungsgericht bestätigte das Urteil des Erstgerichts und führte ergänzend aus, dass § 152 Abs 1 GewO keinesfalls als gesetzlicher Auftrag zur Datensammlung verstanden werden könne.⁴⁹⁹

Hinsichtlich der Öffentlichkeit führte der OGH ergänzend aus, dass die DSK bereits in einer Empfehlung vom 29.11.2005⁵⁰⁰ „zu einem vergleichbaren Sachverhalt, in dem jedermann gegen ein Entgelt von EUR 25,00 von einer Datenbank Bonitätsinformationen einholen konnte, die öffentliche Zugänglichkeit und damit die Anwendbarkeit des § 28 Abs 2 DSG bejaht hat.“⁵⁰¹

Kritisiert wurde von *Knyrim*, dass eine systematische Einordnung von vorab kontrollpflichtigen Kreditauskunfteien iSd § 18 Abs 2 Z 3 unter § 28 Abs 2 DSG unmöglich sei, da bei Kreditauskunfteien stets eine Interessenabwägung notwendig sei, weil es sich um besonders „heikle“ Datenanwendungen handle, keinesfalls aber um „harmlose“ Verzeichnisse iSd § 28 Abs 2 DSG.⁵⁰² Verfassungskonform müsse § 28 Abs 2 DSG mittels § 1 Abs 2 DSG interpretiert werden, der bei Eingriffen in das Grundrecht eine Interessenabwägung vorsehe.⁵⁰³ § 28 Abs 2 DSG sei teleologisch auf „Register und Verzeichnisse“ zu reduzieren.⁵⁰⁴

⁴⁹⁶ OGH 01.10.2008, 6 Ob 195/08g, Seite 6.

⁴⁹⁷ OGH 01.10.2008, 6 Ob 195/08g, Seite 6.

⁴⁹⁸ OGH 01.10.2008, 6 Ob 195/08g, Seite 6.

⁴⁹⁹ OGH 01.10.2008, 6 Ob 195/08g, Seite 7.

⁵⁰⁰ DSK 29.11.2005, K 211.593/0011-DSK/2005.

⁵⁰¹ OGH 01.10.2008, 6 Ob 195/08g, Seite 9 f.

⁵⁰² Vgl *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060 (1061).

⁵⁰³ *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060 (1061).

⁵⁰⁴ *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060 (1061).

Auch Art 14 der RL 1995/46/EG sähe entweder eine Ausnahme vom Widerspruchsrecht vor, oder eine Erweiterung des Widerspruchsrechts, diesfalls nur mit Interessenabwägung. Ein Widerspruch ohne Interessenabwägung werde nur im Bereich des Direktmarketings vorgesehen, weshalb die Vereinbarkeit von § 28 Abs 2 DSG mit der RL fraglich sei.⁵⁰⁵ Auch die Bejahung der Öffentlichkeit sieht *Knyrim* kritisch.⁵⁰⁶

Meines Erachtens zeigt diese Diskussion einmal mehr, dass das Datenschutzrecht eine besonders komplexe und nicht leicht verständliche Materie ist.⁵⁰⁷ Das Zusammenspiel des österr DSG mit den europarechtlichen Vorgaben, vor allem der RL 1995/46/EG, sowie die verfassungskonforme Interpretation eröffnen auf mehrere Bestimmungen des DSG einen neuen Blick. In diesem Zusammenhang ist meiner Ansicht nach besonders interessant, wie weit die Regelung „dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung“⁵⁰⁸ dem einzelnen Mitgliedstaat ein Abweichen von Art 14 der RL 1995/46/EG ermöglicht. Wenn diese Abweichmöglichkeit eng verstanden wird, ist tatsächlich fraglich, inwieweit abseits von Direktwerbung⁵⁰⁹ ein gültiger Widerspruch ohne Interessenabwägung erfolgen kann. Wenn davon ausgegangen wird, dass § 28 Abs 2 DSG eine für den Betroffenen zu großzügige Widerspruchsmöglichkeit geschaffen hat, hätte jeweils eine Interessenabwägung iSd § 28 Abs 1 DSG zu erfolgen. Da jedoch im konkreten Fall die Angabe des Betrages, für den Exekution bewilligt wurde, fehlt, kann schwer nachvollzogen werden, inwiefern das Gläubigerinteresse am Eintrag des Datensatzes dem Interesse des Betroffenen auf Nichteintragung überwiegt.

In diesem Zusammenhang werde ich die ebenso fragwürdige Umsetzung des § 8 Abs 1 Z 4 DSG zur Interessenabwägung erwähnen: Dort heißt es, dass schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten dann nicht verletzt sind, „wenn überwiegende berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern“⁵¹⁰. Art 7 lit f der Datenschutzrichtlinie schreibt jedoch vor, dass die Verarbeitung personenbezogener Daten erfolgen darf, wenn die Verarbeitung zur

⁵⁰⁵ *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060 (1061).

⁵⁰⁶ Er vergleicht den Begriff der Öffentlichkeit auch mit anderen Gesetzen und kommt zum Schluss, dass es keinen einheitlichen oder definierten Begriff dafür gibt - *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060 (1062).

⁵⁰⁷ Ähnliche Schlussfolgerungen zum Datenschutzrecht im Zusammenhang mit klinischen Prüfungen ziehen *Hönel/Raschauer/Wessely*: *Hönel/Raschauer/Wessely*, Datenschutzrechtliche Fragestellungen im Zusammenhang mit klinischen Prüfungen, *RdM* 2006, 106 (114).

⁵⁰⁸ Art 14 lit a der RL 1995/46/EG.

⁵⁰⁹ Vgl Art 14 lit b der RL 1995/46/EG.

⁵¹⁰ § 8 Abs 1 Z 4 DSG.

Verwirklichung des berechtigten Interesses erforderlich ist, „das von dem für die Verarbeitung Verantwortlichen oder von dem bzw den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Abs 1 (der RL 1995/46/EG, Anm) geschützt sind, überwiegen⁵¹¹“⁵¹². Die RL sieht somit vor, dass die Verarbeitung solange erfolgen darf, als nicht das Interesse oder die Grundrechte und Grundfreiheiten des Betroffenen überwiegen. Die österr Bestimmung erfordert hingegen überwiegende Interessen des Auftraggebers oder eines Dritten.⁵¹³ Nach der RL wäre somit bei gleichem Wiegen der beiderseitigen Interessen eine Verarbeitung bzw Verwendung (iSd österr Terminologie) zulässig. Die österr Bestimmung erfordert hingegen ein Überwiegen des Interesses des Auftraggebers oder eines Dritten.⁵¹⁴

Die österr Umsetzung der RL ist somit mE gerade im Bereich der Verwendung von personenbezogenen Daten in mehrerlei Hinsicht zu hinterfragen.

OGH 17.12.2009, 6 Ob 247/08d⁵¹⁵:

In diesem Verfahren wurde vom Kläger eine Entschädigung wegen erlittener Kränkung von EUR 750,00 begehrt, weil die Beklagte bonitätsrelevante Daten veröffentlicht habe, wodurch das Ansehen untergraben oder zumindest erschüttert wurde.⁵¹⁶ Der Betroffene hat seinen Anspruch an einen Konsumentenschutzverein abgetreten, der das Verfahren als Kläger geführt hat.

Zum Grund der Eintragung in der Bonitätsdatenbank: Der Betroffene besitzt ein Ferienhaus an einem See. Eines Tages erhielt er von einem Bewachungsunternehmen, das von den Gemeinden rund um den See mit der Überwachung von Müllplätzen beauftragt war, eine Verschreibung über EUR 100,00 als Unkostenbeitrag zur Abfallbeseitigung, mit der Begründung, er habe einen Verstoß gegen das Abfallwirtschaftsgesetz dadurch begangen,

⁵¹¹ In der Datenschutzrichtlinie heißt es „überwiesen“, wobei es sich hierbei um einen orthographischen Fehler handeln muss, da die dazu bestehende Literatur stets von „überwiegen“ sprechen, zB *Jahnel*, Handbuch Datenschutzrecht, 4/37.

⁵¹² Art 7 lit f der RL 1995/46/EG.

⁵¹³ Zur Frage der nicht korrekten Umsetzung von Richtlinien, deren Überprüfung durch die EK sich über mehrere Jahre ziehen kann: *Mütsch*, Kreditwirtschaftlich wichtige Vorhaben der EU, Kreditwesen 1997, 1058 (1058).

⁵¹⁴ Vgl auch *Jahnel*, Handbuch Datenschutzrecht, 4/37 f.

⁵¹⁵ Vgl OGH 17.12.2009, 6 Ob 247/08d.

⁵¹⁶ Vgl OGH 17.12.2009, 6 Ob 247/08d, Seite 4.

dass er Müll neben Müllcontainern abgelagert habe.⁵¹⁷ Da der Betroffene diesen Vorwurf als nicht gerechtfertigt erachtete, zahlte er nicht. Auf mehrere Zahlungsaufforderungen eines Inkassounternehmens reagierte er mit einem Anruf, in dem er mitteilte, dass diese Forderung nicht berechtigt sei und er nur nach einer erfolgreichen Klagsführung zahlen werde. Daraufhin erfolgte der negative Vermerk in der Bonitätsdatenbank des Inkassounternehmens.

Als der Betroffene für seinen 14-jährigen Sohn einen Mobiltelefonvertrag abschließen wollte, lehnte das Mobiltelefonieunternehmen nach einer Einsicht in die Datenbank der Beklagten den Vertragsabschluss ab.

Das Erstgericht gab dem Klagebegehren mit dem Hinweis auf die rechtswidrige Aufnahme in die Datenbank, weil der Betroffene hievon nicht verständigt worden sei, statt. Auch wurde die Datenbank der Beklagten als öffentlich zugängliche Datei qualifiziert, weil sie einem nicht von vornherein bestimmten, nach außen hin nicht begrenzten Personenkreis zugänglich gemacht werde und der Zugang zur Datei nur von der Entscheidung des Auftraggebers über das ausreichende „berechtigte“ Interesse des Abfragers abhängig sei.⁵¹⁸ Unter Berücksichtigung der beruflichen Tätigkeit des Betroffenen⁵¹⁹ und der vom Betroffenen angestellten Nachforschungen mit einem nicht bloß unerheblichem Zeitaufwand, sei die Eintragung geeignet, das berufliche Fortkommen zu gefährden und zu beeinträchtigen, da potentielle Geschäftspartner mit Sicherheit Personen, deren Kreditwürdigkeit in Frage stehe, meiden würden.

Das Berufungsgericht bestätigte das erstinstanzliche Urteil und verwies darauf, dass der Begriff des höchstpersönlichen Lebensbereichs iSd § 7 MedienG auf jeden Fall die in § 33 Abs 1 zweiter Satz iVm § 18 Abs 2 Z 1 bis 3 DSG normierten Voraussetzungen für den Entschädigungsanspruch wegen der erlittenen Kränkung durch Bloßstellung abdecke. Auch das Erfordernis eines Benutzerkontos und eines Passworts könnten die Eigenschaft der Öffentlichkeit der Bonitätsdatenbank nicht aufheben.⁵²⁰

Der OGH sprach aus, dass die Revision der beklagten Partei entgegen dem Ausspruch des Berufungsgerichts nicht zulässig sei, da keine erhebliche Rechtsfrage vorliege, weil klare

⁵¹⁷ Vgl OGH 17.12.2009, 6 Ob 247/08d, Seite 3.

⁵¹⁸ Vgl OGH 17.12.2009, 6 Ob 247/08d, Seite 6.

⁵¹⁹ Dieser war Geschäftsführer einer GmbH in Wien, die sich mit Unternehmensberatungen befasst.

⁵²⁰ Vgl OGH 17.12.2009, 6 Ob 247/08d, Seite 7.

Rechtsprechung bereits vorliege und keine Gründe für ein Abgehen hiervon ersichtlich sind. So wurden etwa folgende Bereiche vom OGH genannt:

- Der Anspruch auf angemessene Entschädigung wegen erlittener Kränkung nach § 33 Abs 1 DSGVO.⁵²¹
- Der Begriff „öffentlich zugänglich“ in § 33 Abs 1 DSGVO.⁵²²
- Zur Rechtswidrigkeit, wenn eine Eintragung in eine die Kreditwürdigkeit massiv beeinträchtigende Datenanwendung ohne Benachrichtigung des Betroffenen erfolgt.⁵²³

5. Vergleichbare Systeme in Deutschland

Auch an dieser Stelle werde ich wiederum auf SCHUFA verweisen⁵²⁴, welche über den größten Datenbestand zur Beurteilung des aktuellen Zahlungsverhaltens in Deutschland verfügt.⁵²⁵ SCHUFA sieht sich selbst als Anbieter von kreditrelevanten Informationen⁵²⁶ und betont, dass die jeweilige Entscheidung, ob etwa ein Kreditvertrag mit einer natürlichen Person abgeschlossen wird oder nicht, allein von den beiden Vertragsparteien – vor allem vom Kreditgeber – gefasst werde.⁵²⁷ Ebenso trifft demnach ein Mobilfunkunternehmen bzw der jeweilige Angestellte selbst die Entscheidung, ob es einen Handyvertrag mit jemandem eingeht oder nicht.

Die praktisch sehr hohe Bedeutung von Wirtschaftsauskunfteien machen mE klarere Regeln notwendig, die auch Grenzen der Informationsbereitstellung bonitäts-(ir)relevanter Daten aufzeigen. Hierbei wäre eine in den Mitgliedstaaten der Europäischen Union einheitliche Vorgehensweise sinnvoll. Ich bevorzuge die Schaffung von Bagatellgrenzen, unterhalb derer die Speicherung von positiven, als auch negativen Bonitätseinträgen, nicht erlaubt sein soll. Somit soll sichergestellt werden, dass das mögliche Übersehen von Zahlungsaufforderungen einer Rechnung iHv EUR 20,00 nicht zur beinahe Unmöglichkeit eines Handyvertrages führt. Gleichzeitig muss aber natürlich das Interesse der Unternehmen an grundsätzlich

⁵²¹ OGH 15.12.2005, 6 Ob 275/05t.

⁵²² OGH 01.10.2008, 6 Ob 195/08g und OGH 12.11.2009, 6 Ob 156/09y.

⁵²³ OGH 15.12.2005, 6 Ob 275/05t.

⁵²⁴ Vgl IV.C.5 Vergleichbare Systeme in Deutschland sowie IV.D.5 Vergleichbare Systeme in Deutschland.

⁵²⁵ Jahresbericht 2010 von SCHUFA, Seite 26 -
http://www.schufa.de/media/teamwebservices/unternehmen/downloads/Schufa_JB_2010_de.pdf (Stand: 18.08.2013).

⁵²⁶ <http://www.schufa.de/de/private/unternehmen/unternehmenstartseite.jsp> (Stand: 18.08.2013).

⁵²⁷ <http://www.schufa.de/de/private/unternehmen/unternehmenstartseite.jsp> (Stand: 18.08.2013).

zahlungsfähigen Kunden und ihr Vertrauen darauf gewahrt bleiben. Über die konkrete Höhe müsste ein politischer Konsens gefunden werden. Auch wäre eine Anlehnung an die in Österreich bereits bestehende Grenze, ab der Kleinkredite in der Kleinkreditevidenz gespeichert werden dürfen, denkbar. Derzeit können Positivdaten zu Krediten ab einem Betrag von über EUR 300,00 gespeichert werden. Die Unterscheidung zwischen einem aufgenommenen Kredit und der Absicherung eines tagtäglichen Geschäftes würde eine entsprechende Minderung der Bagatellgrenze erforderlich machen.

Ich sehe unterhalb eines Betrages von EUR 100,00 die Verhältnismäßigkeit eines Negativeintrages in einem Informationsverbundsystems nicht als gewahrt an und spreche mich daher für Bagatellgrenzen auch bei Negativeinträgen aus.

Zudem ist zu betonen, dass Bonitätsauskünfte Eintragungen vornehmen, ohne dass eine rechtskräftige gerichtliche Entscheidung zugrunde liegt. Wenn etwa die Zahlung einer Rechnung verweigert wird, da der Betrag dem Grunde oder der Höhe nach zu Unrecht gefordert wird (wie im Beispiel mit der Müllentsorgung), erfolgt trotzdem eine Eintragung. Ein Abstellen auf rechtskräftige gerichtliche Entscheidungen oder Vergleiche würde mit Sicherheit mehr Rechtssicherheit bringen, aber andererseits den Zweck der Bonitätsauskunft nicht erfüllen, da oft langwierige Verfahren geführt werden müssen. Ein wichtiger Ausgleich dafür ist eine strenge Informationspflicht vor der Eintragung sowie die Möglichkeit zur Anmerkung, dass die Forderung dem Grunde oder der Höhe nach bestritten wird. Im Vergleich zur behandelten Warnliste und zur besprochenen Kleinkreditevidenz sind daher eine gesetzlich vorgesehene Mindestgrenze, eine strenge Informationspflicht vor der Eintragung sowie die Möglichkeit der Anmerkung zum Inhalt der Forderung notwendig.

F. Exkurs: Bank AGB 2000 – mehrere Klauseln unwirksam

1. AGB 1979

Die AGB 1979 waren in mehreren Punkten nicht mehr mit den gesetzlichen Vorgaben konform.⁵²⁸ Die Allgemeinen Geschäftsbedingungen werden jeweils beim Abschluss von Geschäften zugrunde gelegt. Im Folgenden werde ich nur auf die datenschutzrechtlich relevanten Bereiche der Bank AGB 2000 eingehen, die durch die Judikatur des OGH als gesetzwidrig angesehen wurden.

2. „Neue“ Bank AGB 2000

a) Entstehung

Unter fachlicher Begleitung⁵²⁹ wurden die neuen AGB entworfen. Im Kommentar *Iro/Koziol*, Allgemeine Bedingungen für Bankgeschäfte (2001) werden alle durch die AGB 2000 geschaffenen Klauseln als wirksam qualifiziert, wenngleich vereinzelt leichte Skepsis zum Ausdruck gebracht wird.⁵³⁰

b) Verfahren des VKI

Der VKI sah nicht durchwegs die Gesetzkonformität gegeben und erhob eine Unterlassungsklage gegen die Creditanstalt AG⁵³¹ nach § 29 KSchG⁵³², die sich ursprünglich gegen insgesamt 18 Klauseln der neuen AGB richtete.⁵³³ Das OLG Wien erklärte 17 Klauseln für gesetzwidrig.⁵³⁴ „Nach knapp zwei Jahren Prozess hat der OGH (4 Ob 179/02f) nunmehr 12 der beanstandeten Klauseln für gesetzwidrig, fünf hingegen für gesetzeskonform erklärt.“⁵³⁵ Die Z 63 war im Revisionsstadium nicht mehr Gegenstand des Prozesses. Inwiefern diese mit den Vorgaben der Wertpapierdienstleistungsrichtlinie konform ist, ist nicht geklärt. Gegen die klagsabweisende Entscheidung des erstinstanzlichen Gerichts wurde

⁵²⁸ Vgl *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 1 mwN.

⁵²⁹ Vgl Beschreibung im Vorwort zu *Iro/Koziol*, ABB-Kommentar (2001), Seite 5.

⁵³⁰ So zB *Iro* in *Iro/Koziol*, ABB-Kommentar (2001), Z 50, Rz 10, wo der Sicherungscharakter von Pfandrechten an Werten aus Gemeinschaftskonten/-depots auf Ansprüche des Kreditinstituts aus der Geschäftsverbindung mit nur einem der Konto-/Depotinhaber auf „Oder-Konten“ beschränkt wird, sofern die aaO vertretene Ansicht von *Iro* nicht geteilt wird.

⁵³¹ Da die AGB der damaligen Creditanstalt AG weitgehend mit jenen anderer Banken übereinstimmen, hat das Urteil auch für andere Banken Bedeutung.

⁵³² BGBl Nr 140/1979, zuletzt geändert durch BGBl I Nr 50/2013: Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG).

⁵³³ *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 1.

⁵³⁴ OLG Wien 17.04.2002, 1 R 229/01f.

⁵³⁵ *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 1.

keine Berufung durch den VKI erhoben. Dies vermutlich deshalb, „um eine all zu lange Prozessdauer aufgrund einer möglichen Vorlage beim EuGH zu vermeiden“⁵³⁶.

c) Urteil des OGH 4 Ob 179/02f

Insgesamt wurden im Urteil des OGH⁵³⁷ 12 Klauseln für ungültig erklärt. Darunter fanden sich zwei Klauseln, die Bestimmungen zum Datenschutz enthielten. Diese zwei Ziffern werde ich an dieser Stelle kurz darstellen, sowie anschließend die Gründe für die Unwirksamkeit der Bestimmungen erläutern:

(1) Z 26 der Bank AGB 2000

(a) Regelung

Die Bestimmung lautet:

- (1) Der Kunde erklärt sich einverstanden, dass das Kreditinstitut nachstehende Daten an die Kleinkreditevidenz und die Warnliste, die derzeit beim Kreditschutzverband von 1870 eingerichtet sind, übermittelt: Name, Anschrift, Geburtsdatum, Höhe der Verbindlichkeit, Rückführmodalitäten, Schritte des Kreditinstituts im Zusammenhang mit der Fälligestellung und der Rechtsverfolgung sowie den Missbrauch von Zahlungsverkehrsinstrumenten. Zweck der Übermittlung ist die Verwahrung, Zusammenführung und Weitergabe der vorstehend angeführten Daten durch den Empfänger an andere Kreditinstitute, Leasinggesellschaften und andere Finanzinstitute und Versicherungsunternehmen zur Wahrung ihrer Gläubigerschutzinteressen.*
- (2) Der Kunde erklärt sich auch damit einverstanden, dass den Kunden oder ein mit ihm konzernmäßig verbundenes Unternehmen betreffende Daten, die dem Kreditinstitut im Rahmen der Geschäftsverbindung mit dem Kunden bekannt geworden und zur Beurteilung der aus Geschäften mit der jeweils betroffenen Person oder Gesellschaft entstehenden Risiken notwendig oder zweckmäßig sind (insbesondere Bilanzdaten), an*
- (potenzielle) Konsortial-/Risikopartner des Kreditinstituts zur Risikobeurteilung im Rahmen des Konsortialgeschäfts,*
 - Refinanzierungsgeber des Kreditinstituts, denen gegenüber die Forderungen des Kreditinstituts gegen den Kunden als Sicherheit dienen sollen (insbesondere Österreichische Nationalbank, Österreichische Kontrollbank*

⁵³⁶ Vgl Graf, Jetzt schlägt's aber (fast) 13!, ecolex-Script 2003/24, 1 mit Verweis auf die FN 6 aaO.

⁵³⁷ OGH 19.11.2002, 4 Ob 179/02f, VRInfo 2003 H 1, 4 et altera.

AG, Europäische Zentralbank, Europäische Investitionsbank), zur Beurteilung der bestellten Sicherheiten,

- *Einlagen- und Anlegerentschädigungseinrichtungen des Fachverbandes, dem das Kreditinstitut angehört, im Rahmen eines Frühwarnsystems zur Beurteilung allfälliger von diesen Einrichtungen abzudeckenden Risiken weitergegeben werden.*⁵³⁸

(b) Hintergründe zur Bestimmung

Durch Z 26 Abs 1 stimmt der Kunde der Weitergabe bestimmter ihn betreffender Daten an die Kleinkreditevidenz und die Warnliste zu. Dadurch sollen Gläubigerinteressen anderer Kreditinstitute, von Leasinggesellschaften und anderer Finanzinstitute, und von Versicherungsunternehmen gewahrt werden.

In Z 26 Abs 2 „erklärt sich der Kunde damit einverstanden, dass das Kreditinstitut an Geschäftspartner, wie zB Konsortialpartner, Daten des Kunden weiterleitet, die zur Risikobeurteilung notwendig oder zweckmäßig sind.“⁵³⁹

Grundsätzlich muss eine konkrete Datenanwendung gemäß § 7 DSGVO zwei Voraussetzungen erfüllen:⁵⁴⁰

- 1) Der Zweck und Inhalt der Datenanwendung muss von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sein.
- 2) Schutzwürdige Geheimhaltungsinteressen der Betroffenen dürfen nicht verletzt werden.

Bei einer Übermittlung müssen die in § 7 Abs 2 DSGVO zusätzlich genannten Erfordernisse erfüllt werden.⁵⁴¹

Wann schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten nicht verletzt werden, umschreibt § 8 DSGVO. Nach § 8 Abs 1 Z 2 DSGVO werden schutzwürdige Geheimhaltungsinteressen dann nicht verletzt, wenn „der Betroffene der Verwendung seiner

⁵³⁸ Vgl Graf, Jetzt schlägt's aber (fast) 13!, ecolo-Script 2003/24, 5.

⁵³⁹ Graf, Jetzt schlägt's aber (fast) 13!, ecolo-Script 2003/24, 5.

⁵⁴⁰ Vgl § 7 Abs 1 DSGVO.

⁵⁴¹ Vor allem müssen die übermittelten Daten aus einer gemäß Abs 1 zulässigen Datenanwendung stammen und muss die ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft gemacht werden (§ 7 Abs 2 Z 1 und 2 DSGVO); vgl auch Pollirer/Weiss/Knyrim, DSGVO (2010) § 7 ErläutRV.

Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt“⁵⁴². Andere Zulässigkeitsgründe werden in § 8 Abs 1 DSGVO genannt.

(c) Gründe für die Unwirksamkeit der Bestimmung

Nach Ansicht des OGH verstößt die Z 26 der Bank AGB 2000 gegen das Transparenzgebot des § 6 Abs 3 KSchG. „Die Klausel entspricht – so der OGH – deswegen nicht den Vorgaben des Transparenzgebotes, weil sie es unterlässt, den Kunden über die nach § 8 Abs 1 Z 2 DSGVO gegebene Möglichkeit, die Zustimmungserklärung jederzeit zu widerrufen, aufzuklären.“⁵⁴³

Die Widerrufsmöglichkeit wird somit als ein zentraler Bestandteil des aus der Zustimmung des Betroffenen folgenden Schutzes angesehen. Die Bestimmung der Bank AGB 2000 vermittelt dem Verbraucher ein unklares Bild seiner vertraglichen Position. Die Kenntnis der Widerrufsmöglichkeit kann nicht vorausgesetzt werden.⁵⁴⁴

Der OGH wendet hierbei die Grundsätze der deutschen Judikatur zum Transparenzgebot an, nach der „aus dem Transparenzgebot eine Verpflichtung des durch die AGB die Rechtslage zu seinen Gunsten verändernden Unternehmers folgt, den Verbraucher wahrheitsgemäß und vollständig über die nunmehr bestehende Rechtslage aufzuklären“⁵⁴⁵. Eine generelle Pflicht, den Vertragspartner über alle ihm nach dem Gesetz zustehenden Rechte zu informieren, besteht jedoch nicht.⁵⁴⁶ Das Fehlen eines Hinweises auf das Widerspruchsrecht nach § 28 DSGVO wirkt sich auf die Zulässigkeit der Klausel nicht aus. Entscheidend ist, dass der Betroffene nicht über die durch § 8 Abs 1 Z 2 DSGVO eingeräumte Möglichkeit informiert wird, „eine bereits erteilte Zustimmung zur Datenweitergabe zu widerrufen“⁵⁴⁷. Dies verletzt das aus § 6 Abs 3 KSchG abgeleitete Transparenzgebot sowie auch den im § 6 Abs 1 Z 1 DSGVO festgelegten Grundsatz, wonach Daten „nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden dürfen“.⁵⁴⁸ Kritisch äußerte sich dazu *Iro*, der für diese Ansicht keinen Anhaltspunkt im Gesetz findet und die Pflicht zur Information des Betroffenen selbst

⁵⁴² § 8 Abs 1 Z 2 DSGVO.

⁵⁴³ *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 5.

⁵⁴⁴ *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 6 mwN, vor allem zur Frage, ob überwiegende berechnete Interessen des Auftraggebers die Verwendung erfordern und somit die Verwendung bereits aufgrund von § 39 Abs 2 BWG in Zusammenhang mit § 8 Abs 1 Z 4 DSGVO rechtmäßig erfolge (FN 29 aaO).

⁵⁴⁵ *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 6 (FN 30) mit Verweis auf *Brandner* in *Ulmer/Brandner/Hensen*, *AGB-Gesetz*⁹ (2001), § 9 ABGB, Rz 87 ff.

⁵⁴⁶ Vgl *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (146).

⁵⁴⁷ *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (146).

⁵⁴⁸ Vgl *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (146) mit Verweis auf § 6 Abs 1 Z 1 DSGVO.

für einen den üblichen Interpretationsgrundsätzen verhafteten Juristen als schwerlich nachvollziehbar erachtet.⁵⁴⁹

Tatsächlich ist die Grenzziehung, über welche gesetzlichen Bestimmungen der Betroffene in den AGB informiert werden muss und welche Normen nicht erwähnt werden müssen, im Einzelfall schwierig. Dass etwa über die Möglichkeit zum Widerruf gem § 8 Abs 1 Z 2 DSG informiert werden muss und über das Widerspruchsrecht gem § 28 DSG nicht, ist mE erst nach der ergangenen Entscheidung für den Anwender zweifelsfrei klargelegt. Im Ergebnis ist die Entscheidung hinzunehmen. Als wesentliches Argument kann vorgebracht werden, dass sich im gleichen Satz, in dem die Zustimmung des Betroffenen zur Verwendung seiner nicht-sensiblen Daten als Wahrung der schutzwürdigen Geheimhaltungsinteressen gesehen wird, auch die Erwähnung der Widerrufsmöglichkeit findet und dass somit eine Klausel, welche nur den ersten Teil der Bestimmung wiedergibt, unvollständig über die Rechte des Betroffenen informiert.

(2) Z 27 der Bank AGB 2000

(a) Regelung

Die Bestimmung lautet:

In den in Z 26 genannten Fällen entbindet der Kunde das Kreditinstitut ausdrücklich vom Bankgeheimnis.

(b) Hintergründe zur Bestimmung

Wenn der Kunde der Offenbarung eines Geheimnisses ausdrücklich und schriftlich zustimmt, besteht gemäß § 38 Abs 2 Z 5 BWG die Verpflichtung zur Wahrung des Bankgeheimnisses nicht. Fraglich ist, ob eine Bestimmung in den Bank AGB einer ausdrücklichen und schriftlichen Zustimmung entspricht.

Nach *Koziol* ist dem Erfordernis des § 38 Abs 2 Z 5 BWG dann Genüge getan, wenn die Zustimmung in den AGB enthalten ist und darauf in einem schriftlich unterfertigten Kontoeröffnungsvertrag hingewiesen wird, sofern der Hinweis ausreichend deutlich ist.⁵⁵⁰

Aus dem BWG ergäbe sich nämlich keineswegs, dass die Unterschrift unbedingt auf dem Papier zu erfolgen habe, auf dem die AGB abgedruckt seien, weswegen auch eine gesonderte,

⁵⁴⁹ *Iro*, OGH: Unwirksame Klauseln in den Allgemeinen Geschäftsbedingungen der Banken, RdW 2003, 66 (67).

⁵⁵⁰ *Koziol* in *Iro/Koziol*, ABB-Kommentar (2001), Z 27, Rz 2 und 3.

unterschiedene Urkunde genüge, in welcher der Kunde das Einverständnis mit der Geltung der AGB erklärt.⁵⁵¹

(c) Gründe für die Unwirksamkeit der Bestimmung

Der OGH hat in der Entscheidung 4 Ob 28/01y⁵⁵² bereits klargestellt, „dass die Aufnahme der Klausel in – regelmäßig nicht unterfertigte – AGB nicht für eine (wirksame) Entbindung vom Bankgeheimnis ausreiche“⁵⁵³. Die geforderte Ausdrücklichkeit setzt voraus, dass die Entbindungserklärung klar und deutlich im unterfertigten Schriftstück enthalten ist.⁵⁵⁴

Wirksam wäre eine Entbindung vom Bankgeheimnis, wenn die Klausel in die vom Kunden ohnehin zu unterfertigenden Vertragsformblätter aufgenommen wird.⁵⁵⁵

Die Unwirksamkeit der Regelung Z 27 der Bank AGB 2000 wird vom OGH ausschließlich auf § 38 Abs 2 Z 5 BWG gestützt, ohne dass das Transparenzgebot in diesem Zusammenhang erwähnt wird. Das ist in Anlehnung an *Graf* sehr zu begrüßen, da die Unzulässigkeit einer Entbindung vom Bankgeheimnis in AGB unzweifelhaft aus dieser Norm selbst und nicht erst aus dem Transparenzgebot folgt.⁵⁵⁶

Apathy vergleicht § 38 Abs 2 Z 5 BWG mit der damals in § 577 Abs 3 ZPO⁵⁵⁷ geregelten Formvorschrift, wonach der Schiedsvertrag schriftlich errichtet werden oder in Telegrammen, Fernschreiben oder elektronischen Erklärungen enthalten sein muss, die die Parteien gewechselt haben.⁵⁵⁸ Daraus wurde im Schrifttum der Schluss gezogen, dass die Urkunde, welche die formpflichtige Erklärung einer Schiedsgerichtsklausel enthält, jedenfalls der unterschriebenen Urkunde beigelegt sein muss. Der durch das Schiedsrechts-Änderungsgesetz 2006⁵⁵⁹ neu geregelte § 583 ZPO brachte für den Bereich der Schiedsvereinbarung eine Klarstellung der erforderlichen Form und akzeptiert Schiedsvereinbarungen in gewechselten Schreiben, Telefaxen, E-Mails oder anderen Formen der Nachrichtenübermittlung, die einen Nachweis der Vereinbarung sicherstellen.⁵⁶⁰

⁵⁵¹ *Koziol in Iro/Koziol*, ABB-Kommentar (2001), Z 27, Rz 3.

⁵⁵² OGH 22.03.2001, 4 Ob 28/01y (ÖBA 2001, 645 = *ecolex* 2001/147).

⁵⁵³ *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (147).

⁵⁵⁴ Vgl bereits OGH 29.01.1997, 7 Ob 2299/96f (= ÖBA 1997, 632).

⁵⁵⁵ *Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141 (147).

⁵⁵⁶ Vgl *Graf*, Jetzt schlägt's aber (fast) 13!, *ecolex-Script* 2003/24, 6.

⁵⁵⁷ § 577 Abs 3 ZPO idF BGBl I Nr 152/2001.

⁵⁵⁸ Vgl *Apathy*, Die neuen ABB auf dem Prüfstand – Anmerkungen zu OGH 4 Ob 179/02f, ÖBA 2003, 177 (183).

⁵⁵⁹ BGBl I Nr 7/2006: Bundesgesetz, mit dem in der Zivilprozessordnung das Schiedsverfahren neu geregelt wird sowie das Einführungsgesetz zur Jurisdiktionsnorm, das Einführungsgesetz zur Zivilprozessordnung, das Arbeits- und Sozialgerichtsgesetz, das Gerichtsorganisationsgesetz und das Richterdienstgesetz geändert werden (Schiedsrechts-Änderungsgesetz 2006 - SchiedsRÄG 2006).

⁵⁶⁰ Vgl § 583 ZPO idF BGBl I Nr 7/2006.

V. Datenschutzrechtliche Hintergründe

A. Österreichisches Datenschutzgesetz (DSG)

In meiner Dissertation werde ich nur sehr kurz auf allgemeine Grundlagen des Datenschutzgesetzes eingehen, da hierzu bereits umfangreiche Literatur⁵⁶¹ besteht. Zu allgemeinen Problemen des Datenschutzrechtes in Österreich sei *Knyrim*⁵⁶² empfohlen, der darin besonders auf die Vorteile der Selbstregulierung eingeht, sofern ein sinnvoller und effektiver regulativer Rahmen besteht.⁵⁶³ In diesem Kapitel werde ich besonders auf die für die Verwendung und Überlassung von Daten innerhalb von Österreich, der Europäischen Union und gegenüber Drittstaaten relevanten Bestimmungen eingehen und versuchen, Interpretationsschwierigkeiten zu klären.

1. Datenschutzrecht in Österreich

Nachdem Schweden bereits 1973 und Deutschland 1977 ein Datenschutzgesetz normierten⁵⁶⁴, wurde auch in Österreich 1978 ein Datenschutzgesetz⁵⁶⁵ erlassen, welches mit 1. Jänner 1980 in Kraft trat⁵⁶⁶ und damals als Gesetz gesehen wurde, das contra administrationem die Hinterfragung traditioneller Strukturen erzwingt und neue Gestaltungs- und Entscheidungsformen verlangt.⁵⁶⁷ Die Entwicklung wurde auch durch das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten⁵⁶⁸ beeinflusst, wobei an der Ausarbeitung der Konvention österreichische Experten maßgeblich beteiligt waren.⁵⁶⁹ Anfang der 90er Jahre hatten bereits die meisten Mitgliedstaaten der Europäischen Union Datenschutzregelungen erlassen, woraufhin Harmonisierungsbestrebungen auf europäischer Ebene folgten, welche nach mehrjährigen

⁵⁶¹ Vgl etwa *Graf*, Datenschutzrecht im Überblick² (2010), *Jahnel*, Handbuch Datenschutzrecht sowie *Sonntag*, Einführung in das Internetrecht.

⁵⁶² *Knyrim*, 25 Jahre Datenschutzrecht in Österreich – Bestandsaufnahme und Lösungsansätze für aktuelle Probleme, MR 2005, 415.

⁵⁶³ *Knyrim*, 25 Jahre Datenschutzrecht in Österreich – Bestandsaufnahme und Lösungsansätze für aktuelle Probleme, MR 2005, 415 (419 f).

⁵⁶⁴ Vgl *Kobrin*, The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance, S 12 (November 2002) = <http://knowledge.wharton.upenn.edu/papers/1080.pdf> (Stand: 18.08.2013).

⁵⁶⁵ BGBl Nr 565/1978: Datenschutzgesetz.

⁵⁶⁶ § 58 DSG 1978, wobei die Absätze 2 bis 14 leg cit für einzelne Bestimmungen andere Zeitpunkte des Inkrafttretens vorsahen.

⁵⁶⁷ *Stadler*, Das österreichische Datenschutzgesetz als Markstein der Verfassungspolitik und des Informationsrechtes, JBl 1979, 358 (358).

⁵⁶⁸ Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr 108) – vgl auch <http://conventions.coe.int/treaty/ger/treaties/html/108.htm> (Stand: 18.08.2013).

⁵⁶⁹ Vgl *Wittmann*, Die Datenschutzkonvention des Europarates, EDVuR 1989, 96 (96 ff).

Verhandlungen mit der Datenschutzrichtlinie⁵⁷⁰ vorerst endeten. Durch den Beitritt Österreichs zur Europäischen Union am 1.1.1995 wurde Österreich zur Umsetzung der in der RL 1995/46/EG vorgesehenen Ziele verpflichtet, was schließlich im DSG 2000 geschah.

Novellierungen erfolgten mehrmals⁵⁷¹, wobei besonders folgende Änderungen hervorzuheben sind: Regelung für die Verwendung von Daten im Katastrophenfall⁵⁷² und die umfangreiche DSG-Novelle 2010⁵⁷³ mit zahlreichen Definitionsänderungen bzw -klarstellungen und ua einem neuen Abschnitt 9a zur Videoüberwachung.

2. Verwendung von Daten

Im Anschluss an die bereits erfolgte Begriffsbestimmung im zweiten Kapitel ist zwischen Verwendung und Überlassung von Daten zu unterscheiden. Verwendung bezeichnet im österr DSG einen Überbegriff für Übermittlung und jede andere Art der Verarbeitung von Daten.

Die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses entspricht nach der Legaldefinition in § 4 Z 11 DSG dem Überlassen von Daten.

Es ergeben sich somit folgende Begriffsunterscheidungen:

- Übermittlung von Daten⁵⁷⁴ (= Verwendung von Daten):

Wenn Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister weiter gegeben werden, liegt eine Übermittlung von Daten vor. Darunter fallen insbesondere die Veröffentlichung von Daten, sowie auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

- Verarbeitung von Daten⁵⁷⁵ (= Verwendung von Daten):

Zur Verarbeitung von Daten zählen die Ermittlung, Erfassung, Speicherung, Aufbewahrung, Ordnung, Vergleichung, Veränderung, Verknüpfung, Vervielfältigung, Abfragung, Ausgabe, Benützung, Überlassung, Sperrung, Löschung, Vernichtung oder jede andere Art der Handhabung von Daten mit Ausnahme der Übermittlung von Daten.

⁵⁷⁰ RL 1995/46/EG vom 24. Oktober 1995 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl L 281 vom 23.11.1995, S 31-50).

⁵⁷¹ Novellierungen wurden in folgenden Bundesgesetzblättern publiziert: BGBl I Nr 136/2001, BGBl I Nr 13/2005, BGBl I Nr 2/2008, BGBl I Nr 133/2009, BGBl I Nr 135/2009 und BGBl I Nr 112/2011.

⁵⁷² BGBl I Nr 13/2005.

⁵⁷³ BGBl I Nr 133/2009.

⁵⁷⁴ § 4 Z 12 DSG.

⁵⁷⁵ § 4 Z 9 DSG.

- Überlassung von Daten⁵⁷⁶ (= Verwendung von Daten):

Eine Überlassung von Daten liegt vor, wenn Daten zwischen dem datenschutzrechtlichen Auftraggeber und dem Dienstleister im Rahmen des Auftragsverhältnisses weitergegeben werden.

Wenn personenbezogene Daten durch Österreich nur durchgeführt werden, ist das DSG nicht anwendbar.⁵⁷⁷ Der Begriff der Durchfuhr ist weder im DSG noch in der RL 1995/46/EG definiert.⁵⁷⁸ *Jahnel* verweist auf die E-Commerce-Richtlinie⁵⁷⁹, die in Art 12 den Begriff „reine Durchleitung“ verwendet.⁵⁸⁰

Art 12 Abs 1 der RL 2000/31/EG umschreibt einen Dienst der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln. Der Diensteanbieter ist nicht für die übermittelten Informationen verantwortlich, wenn er die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht auswählt und die übermittelten Informationen nicht auswählt oder verändert. Liegen all diese Merkmale vor, handelt es sich um eine „reine Durchleitung“. Charakteristisch ist daher, dass von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt werden oder der Zugang zu einem Kommunikationsnetz vermittelt wird. Zusätzlich darf der Diensteanbieter die Übermittlung nicht veranlassen, den Adressaten der übermittelten Information nicht auswählen und die übermittelten Informationen nicht auswählen oder verändern.

Der Begriff der „reinen Durchleitung“ wird in Art 12 Abs 2 der RL 2000/31/EG erweitert, indem auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen als Übermittlung von Informationen und die Vermittlung des Zugangs im Sinne von Absatz 1 *leg cit* normiert werden. Dies gilt jedoch nur, soweit die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.⁵⁸¹

⁵⁷⁶ § 4 Z 11 DSG.

⁵⁷⁷ Vgl § 3 Abs 3 DSG.

⁵⁷⁸ *Jahnel*, Handbuch Datenschutzrecht, 3/25.

⁵⁷⁹ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt - Richtlinie über den elektronischen Geschäftsverkehr (= ABl L 178 vom 17.07.2000, S 1–16)

⁵⁸⁰ Vgl Überschrift zu Art 12 der RL 2000/31/EG.

⁵⁸¹ Vgl Art 12 Abs 2 der RL 2000/31/EG.

Systematisch gesehen, steht die Regelung zur „reinen Durchleitung“ in der E-Commerce-Richtlinie im Abschnitt 4 – Verantwortlichkeit der Vermittler. In diesem Abschnitt wird die Verantwortlichkeit der Vermittler eingeschränkt. Neben der Bestimmung zur reinen Durchleitung werden auch Sonderbestimmungen zum Caching⁵⁸², zum Hosting⁵⁸³ und in diesem Zusammenhang zum Nichtbestehen einer allgemeinen Überwachungspflicht⁵⁸⁴ normiert. Entscheidend ist, dass der Diensteanbieter in keiner Weise mit der übermittelten Information in Verbindung steht. Er darf somit unter anderem die von ihm übermittelte Information nicht verändern, wobei Eingriffe technischer Art im Verlauf der Übermittlung nicht unter diese Anforderung fallen, da sie die Integrität der übermittelten Informationen nicht verändern.⁵⁸⁵

Jahnel versteht unter der Durchfuhr Übermittlungen, die nicht vom Inland aus veranlasst werden und bei denen keine selbstständige Bestimmung der Übermittlungsempfänger im Inland und keine Auswahl der zu übermittelnden Informationen erfolgt, wie beispielsweise die Tätigkeit von Internet-Providern, sofern sie nicht als Content-Provider (Anbieter von Inhalten) agieren.⁵⁸⁶ Im Anschluss an die automatische kurzzeitige Zwischenspeicherung, die gem Art 12 Abs 2 auch vom Begriff der „reinen Durchleitung“ erfasst wird, sieht *Jahnel* eine kurzfristige Zwischenspeicherung aus technischen Gründen (zB zur Signalverstärkung oder Datenkomprimierung) als zulässig an, wodurch es nicht zur Anwendung des DSG kommt, wenn die Speicherung nicht länger erfolgt, als dies für die Übermittlung personenbezogener Daten erforderlich ist.⁵⁸⁷

Zusammengefasst handelt es sich mE nach bei der Durchfuhr um Übermittlungen, die vom Ausland aus veranlasst werden, und die im Inland nur weiter geleitet werden, ohne dass der Adressat der übermittelten Information ausgewählt wird oder die übermittelte Information ausgewählt oder verändert wird. Zusätzlich ist auch eine kurzfristige Zwischenspeicherung aus technischen Gründen als „Durchfuhr“ anzusehen, sofern die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

⁵⁸² Art 13 der RL 2000/31/EG.

⁵⁸³ Art 14 der RL 2000/31/EG.

⁵⁸⁴ Art 15 der RL 2000/31/EG.

⁵⁸⁵ Vgl 43. Erwägungsgrund der RL 2000/31/EG.

⁵⁸⁶ *Jahnel*, Handbuch Datenschutzrecht, 3/25; Er verweist auf *Drobesch/Grosinger*, Datenschutzgesetz, Anm zu § 3 Abs 3, 107 und *Dohr/Pollirer/Weiss/Knyrim*, DSG², § 3 Anm 4, 57.

⁵⁸⁷ Vgl *Jahnel*, Handbuch Datenschutzrecht, 3/25.

Somit dürfte Klarheit über die im Zusammenhang mit der Verwendung von Daten bedeutsamen Terminologien im DSG bestehen, wenngleich einzelne Begriffe (zB „nicht länger, als es für die Übermittlung erforderlich ist“) erst bei Kenntnis der genauen technischen Abläufe erschlossen werden können. Der Vorteil dieser Formulierung ist jedoch, dass bei besser werdender Technik keine neuen Regelungen erforderlich sind.

Im Folgenden werde ich nun darauf eingehen, wie eine Datenverwendung in Österreich, sowie die Datenübermittlung und -überlassung in den EWR und in Drittstaaten vor sich geht und was dabei zu beachten ist, damit diese rechtmäßig erfolgt.

3. Datenverwendung in Österreich

a) Allgemeines

Da unter die Verarbeitung jede Art der Handhabung von Daten⁵⁸⁸ mit Ausnahme des Übermittels von Daten fällt, und auch § 7 in den Absätzen 1 und 2 Regelungen für die Zulässigkeit der Verarbeitung⁵⁸⁹ und der Übermittlung⁵⁹⁰ enthält, werde ich auf diese getrennt voneinander eingehen. § 7 Abs 3 DSG normiert die Zulässigkeit der Datenverwendung und umfasst somit sowohl die Verarbeitung, als auch die Übermittlung von Daten.

Wie ich noch erläutern werde, ist im Prüfungsverfahren, ob eine Verarbeitung oder Übermittlung zulässig ist, auch zu prüfen, ob schutzwürdige Geheimhaltungsinteressen verletzt werden. Bei nicht sensiblen Daten erfolgt die Prüfung nach § 8 DSG und bei sensiblen Daten nach § 9 DSG. Sensible Daten sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.⁵⁹¹ Hierbei handelt es sich um besonders schutzwürdige Daten, weshalb auch § 9 DSG im Vergleich zu § 8 DSG strengere Regelungen enthält. So ist etwa die Aufzählung, wann schutzwürdige Geheimhaltungsinteressen nicht verletzt werden, bei sensiblen Daten taxativ, also abschließend.

⁵⁸⁸ Genannt werden in der Legaldefinition des § 4 Z 9 DSG etwa das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen und Vernichten.

⁵⁸⁹ § 7 Abs 1 DSG.

⁵⁹⁰ § 7 Abs 2 DSG.

⁵⁹¹ Vgl § 4 Z 2 DSG.

b) Verarbeitung

Bei einer Verarbeitung müssen stets die Grundsätze der Verwendung von Daten eingehalten werden, die in § 6 DSGVO geregelt sind, wobei der Gesetzgeber freistellt, ob mit der Prüfung der allgemeinen Grundsätze oder der konkreten Zulässigkeitsvoraussetzungen begonnen wird.⁵⁹² Entsprechend dem Datenschutzgesetz können daher folgende Prüfungsschritte abgeleitet werden:⁵⁹³

- 1) Berechtigung des Auftraggebers.⁵⁹⁴
- 2) Keine Verletzung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen.⁵⁹⁵
- 3) Eingriff in das Grundrecht nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln.⁵⁹⁶
- 4) Einhaltung der Grundsätze des § 6 DSGVO.⁵⁹⁷

Nun möchte ich diese Prüfungsschritte etwas genauer erläutern:

Ad 1) Berechtigung des Auftraggebers:

Der Zweck und Inhalt einer Datenanwendung müssen von den gesetzlichen Zuständigkeiten oder den rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sein. Falls weder eine gesetzliche Zuständigkeit noch eine rechtliche Befugnis des Auftraggebers für den Zweck und Inhalt der Datenanwendung vorliegt, ist die Datenanwendung verboten.⁵⁹⁸ Im öffentlichen Bereich ergibt sich die gesetzliche Zuständigkeit aus den Materiengesetzen des Bundes oder der Länder. Erwähnt sei etwa das unter den Informationsverbundsystemen bereits geschilderte MeldeG.⁵⁹⁹ Die rechtliche Befugnis kann sich im privaten Bereich aus einer Gewerbeberechtigung oder bei Vereinen aus dem Vereinsstatut ableiten lassen, wobei die Rechtsordnung als Gesamtheit heranzuziehen ist.⁶⁰⁰ Bei Informationsverbundsystemen im Bereich der Finanzdienstleistungen⁶⁰¹ hat etwa die Konzession der Kreditinstitute nach dem BWG vorzuliegen.⁶⁰²

⁵⁹² *Jahnel*, Handbuch Datenschutzrecht, 4/6.

⁵⁹³ Vgl. auch *Jahnel*, Handbuch Datenschutzrecht, 4/6.

⁵⁹⁴ § 7 Abs 1 DSGVO.

⁵⁹⁵ Vgl. ebenso § 7 Abs 1 DSGVO.

⁵⁹⁶ § 7 Abs 3 DSGVO.

⁵⁹⁷ Vgl. ebenso § 7 Abs 3 DSGVO.

⁵⁹⁸ Vgl. *Pollirer/Weiss/Knyrim*, DSGVO (2010) § 7 Anm 5.

⁵⁹⁹ Vgl. IV.B Zentrales Melderegister.

⁶⁰⁰ *Pollirer/Weiss/Knyrim*, DSGVO (2010) § 7 Anm 5.

⁶⁰¹ Besprochen habe ich bereits IV.C Warnliste der österreichischen Kreditinstitute und IV.D Kleinkreditevidenz.

⁶⁰² Ausführlich zur Berechtigung des Auftraggebers vgl. *Jahnel*, Handbuch Datenschutzrecht, 4/8 ff.

Ad 2) Schutzwürdige Geheimhaltungsinteressen:

Schutzwürdige Geheimhaltungsinteressen des Betroffenen dürfen bei der Verarbeitung von Daten nicht verletzt werden. § 8 DSG regelt ausführlich, wann schutzwürdige Geheimhaltungsinteressen bei Verwendung von nicht-sensiblen Daten nicht verletzt werden. § 9 DSG normiert abschließend, wann schutzwürdige Geheimhaltungsinteressen bei der Verwendung von sensiblen Daten nicht verletzt werden. Ich werde diese beiden Bestimmungen daher nacheinander behandeln.

§ 8 DSG – Schutzwürdige Geheimhaltungsinteressen bei nicht-sensiblen Daten:

Die Gesetzesbestimmung eröffnet bereits relativ deutlich, wann schutzwürdige Geheimhaltungsinteressen nicht verletzt werden. In § 8 Abs 1 DSG werden vier Fälle genannt, in denen keine Verletzung vorliegt:

- es besteht eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten⁶⁰³
- der Betroffene hat der Verwendung seiner Daten zugestimmt, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt⁶⁰⁴
- lebenswichtige Interessen des Betroffenen erfordern die Verwendung⁶⁰⁵
- überwiegend berechtigte Interessen des Auftraggebers oder eines Dritten erfordern die Verwendung⁶⁰⁶

Zusätzlich bestimmt § 8 Abs 2, dass auch bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten⁶⁰⁷ keine schutzwürdigen Geheimhaltungsinteressen verletzt werden.

Abs 3 leg cit beschreibt genauer, wann überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten vorliegen, wobei die Aufzählung mit „insbesondere“ verbunden ist. Es sind daher auch zusätzliche, in Abs 3 nicht genannte, Gründe möglich, die ein überwiegendes berechtigtes Interesse des Auftraggebers oder eines Dritten vorliegen lassen. Hinzuweisen ist nochmals auf die bereits angesprochene Differenz zu Art 7 lit f der

⁶⁰³ § 8 Abs 1 Z 1 DSG.

⁶⁰⁴ § 8 Abs 1 Z 2 DSG.

⁶⁰⁵ § 8 Abs 1 Z 3 DSG.

⁶⁰⁶ § 8 Abs 1 Z 4 DSG.

⁶⁰⁷ Vgl II.A.2.c) Begriffsbestimmung.

RL 1995/46/EG.⁶⁰⁸ Dort heißt es, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn die Verarbeitung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen (= Auftraggeber) oder von dem bzw den Dritten wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art 1 Abs 1 geschützt sind, überwiegen.⁶⁰⁹ Nach den Vorgaben der Datenschutzrichtlinie wäre somit auch bei gleich wiegenden Interessen des Auftraggebers bzw Dritten und des Betroffenen eine Verwendung iSd österr DSG von personenbezogenen Daten möglich. Das österr DSG erfordert hingegen ein Überwiegen berechtigter Interessen des Auftraggebers oder eines Dritten. *Diese offensichtliche Widersprüchlichkeit müsste im österr DSG korrigiert werden.*

§ 8 Abs 4 DSG regelt die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen und normiert, wann die Verwendung dieser Daten nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen verstößt.

Um zu prüfen, ob bei Informationsverbundsystemen im Finanzdienstleistungsbereich eine der in Abs 3 genannten Voraussetzungen vorliegt, sodass eine Zustimmung des Betroffenen nicht erforderlich wäre, werde ich diese kurz erörtern:

Da es sich bei Kreditinstituten nicht um öffentliche Auftraggeber handelt, können § 8 Abs 3 Z 1⁶¹⁰ und Z 2⁶¹¹ DSG nicht angewendet werden. Bei der Verwendung von Daten für Zwecke steuerrechtlicher Natur, wird diese Bestimmung oder § 8 Abs 1 Z 1 DSG anwendbar sein.

Auch ist ein finanzielles Interesse bzw der Schutz vor Insolvenz kein lebenswichtiges Interesse eines Dritten iSd § 8 Abs 3 Z 3 DSG.⁶¹²

Weiters können die Z 6⁶¹³ und Z 7⁶¹⁴ leg cit ausgeschlossen werden, da es sich hierbei um besondere Fälle handelt, die nicht zu einer allgemeinen Lösung führen können.

⁶⁰⁸ Vgl IV.E.4 Judikatur der österr DSK - OGH 01.10.2008, 6 Ob 195/08g.

⁶⁰⁹ Im Original der RL 1995/46/EG ist – wie bereits vorher angesprochen – „überwiesen“ zu lesen, wobei hiermit nur „überwiegen“ gemeint sein kann.

⁶¹⁰ Die Verwendung von Daten ist für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe.

⁶¹¹ Die Verwendung der Daten durch Auftraggeber des öffentlichen Bereichs geschieht in Erfüllung der Verpflichtung zur Amtshilfe.

⁶¹² Die Verwendung der Daten ist zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich.

⁶¹³ Die Verwendung der Daten hat ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand.

⁶¹⁴ Die Verwendung der Daten ist im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig.

§ 8 Abs 3 Z 5 DSGVO⁶¹⁵ könnte nicht den Betrieb der Datenverwendung als solches, sondern nur die Verwendung der Daten vor einer Behörde rechtfertigen. Hierfür ist jedoch Voraussetzung, dass die Daten bereits rechtmäßig ermittelt wurden.

Es verbleibt somit § 8 Abs 3 Z 4 DSGVO, der schutzwürdige Geheimhaltungsinteressen aus dem Grunde des § 8 Abs 1 Z 4 DSGVO dann nicht als verletzt ansieht, wenn die Verwendung der Daten zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist. Klassisches Beispiel ist etwa das Reisebüro, das Daten des Betroffenen (Kunden) an die Fluglinie bekannt geben muss, damit dieser sein Ticket erhält.⁶¹⁶ Die hiermit vergleichbare Bestimmung der Richtlinie normiert, dass die Verarbeitung lediglich erfolgen darf, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen, erforderlich ist.⁶¹⁷

Die Datenschutzrichtlinie erfasst somit auch die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Personen erfolgen, und ist damit deutlich weiter formuliert als § 8 Abs 3 Z 4 DSGVO. Richtlinienkonform interpretiert muss daher die österreichische Bestimmung auf die Durchführung vorvertraglicher Maßnahmen, die auf Antrag des Betroffenen erfolgen, erweitert werden. Wichtig ist, dass die Verwendung der Daten zur Erfüllung einer vertraglichen Verpflichtung (oder eben der Durchführung vorvertraglicher Maßnahme, die auf Antrag des Betroffenen erfolgen) *erforderlich* ist.

Bedeutsam ist daher die Frage, wie weit diese Erforderlichkeit reicht. Wie *Jahnel* 2010 mit Verweis auf *Knyrim* feststellte, gibt es trotz der Häufigkeit dieses Rechtfertigungsgrundes keine nähere Untersuchung der Reichweite von § 8 Abs 3 Z 4 „und so gut wie keine einschlägige Rsp“⁶¹⁸. Neben der Datenverwendung im Bereich von Reisebüros⁶¹⁹ und Warenversandhäusern⁶²⁰ wurde dieser Rechtfertigungsgrund auch auf die Impfdokumentation eines im Rahmen der Privatwirtschaftsverwaltung tätigen Impfarztes angewandt.⁶²¹ Auch

⁶¹⁵ Die Verwendung der Daten ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig und die Daten wurden rechtmäßig ermittelt.

⁶¹⁶ Vgl *Pollirer/Weiss/Knyrim*, DSGVO (2010) § 8 Anm 13.

⁶¹⁷ Vgl Art 7 lit b der RL 1995/46/EG.

⁶¹⁸ *Jahnel*, Handbuch Datenschutzrecht, 4/47 mit Verweis auf *Knyrim*, Nochmals § 107 TKG 2003: Papierwerbung benachteiligt?, *ecolex* 2005, 257 (258).

⁶¹⁹ ZB die bereits angesprochene Weitergabe von Daten an ein Flugunternehmen.

⁶²⁰ ZB die Weitergabe der Lieferadresse an Spediteure.

⁶²¹ DSK 25.06.2004, K120.877/0017-DSK/2004.

wurde von der DSK in einem Genehmigungsbescheid zur Datenanwendung „Betreuungsinformationssystem über die Gewährleistung der vorübergehenden Grundversorgung für hilfs- und schutzbedürftige Fremde in Österreich“ festgestellt, dass hinsichtlich der darin geführten nicht-sensiblen Daten keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden, da „die Verarbeitung ihrer Daten zur Erfüllung des Betreuungsvertrages erforderlich ist (§ 8 Abs 3 Z 4 DSG), sodass ein überwiegendes berechtigtes Interesse der jeweils zur Betreuung verpflichteten Gebietskörperschaft vorliegt (§ 8 Abs 1 Z 4 DSG)“⁶²². Die nach wie vor sehr beschränkt bestehende Rsp zu diesem Bereich ermöglicht auch mir keine eingehende Untersuchung der Reichweite des § 8 Abs 3 Z 4 DSG. Die Gesetzesmaterialien sprechen lediglich davon, dass in § 8 Abs 3 DSG einige der wichtigsten Fälle angeführt werden, „in welchen durch die Datenverwendung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden, weil es sich um zulässige Eingriffe im Sinne des § 1 Abs 2 DSG handelt.“⁶²³ Dieser Katalog sei in keiner Weise erschöpfend und beschränke sich im Übrigen auf Falltypen, bei welchen die Verletzung schutzwürdiger Geheimhaltungsinteressen immer auszuschließen sei. Bemerkenswert ist in diesem Zusammenhang die Anwendung von § 8 Abs 3 Z 4 DSG auf Umstrukturierungsmaßnahmen⁶²⁴, vor allem die Verwendung⁶²⁵ von Mitarbeiterdaten.⁶²⁶ Hinsichtlich der Verwendung sensibler Daten wird aaO auf § 9 Z 11 DSG verwiesen, ohne jedoch auf die nach dieser Bestimmung erforderlichen „besonderen Rechtsvorschriften“ einzugehen.⁶²⁷ Dass bei der Anwendung dieser Bestimmungen keine datenschutzrechtlichen Bedenken bestehen, kann von mir für den Fall der Änderung des Verwendungszweckes nicht nachvollzogen werden.

Der Empfehlung der Beibehaltung von konkret formulierten Datenschutzklauseln in individuellen Arbeitsverträgen kann ich mich daher nur anschließen. Auch muss erwähnt werden, dass abschließend die Wichtigkeit der Einzelfallbetrachtung datenschutzrechtlicher Problemstellungen betont wird, wodurch bei sensiblen Daten die ausdrückliche Zustimmung des Betroffenen iSd § 9 Z 6 DSG notwendig sein kann.

⁶²² DSG 01.02.2005, K500.974-033/0002-DVR/2005.

⁶²³ Vgl ErläutRV 1613 der Beilagen der XX. GP, Besonderer Teil, Zu § 8 des Entwurfs (S 41).

⁶²⁴ *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 96 (103 f).

⁶²⁵ AaO wird die Datenübermittlung von Mitarbeiterdaten angesprochen.

⁶²⁶ *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 96 (104).

⁶²⁷ Vgl ausführlich dazu: *Brodil*, Datenschutzrechtliche Aspekte der Verwendung von Gesundheitsdaten im Arbeitsverhältnis, *ecolex* 2010, 122 (124 f).

§ 9 DSGVO – Schutzwürdige Geheimhaltungsinteressen bei sensiblen Daten:

§ 9 DSGVO nennt abschließend⁶²⁸ in 13 Ziffern die Fälle, wann schutzwürdige Geheimhaltungsinteressen bei der Verwendung von sensiblen Daten nicht verletzt werden.

§ 9 Z 1 DSGVO⁶²⁹ hat gerade in sozialen Netzwerken⁶³⁰ eine große Bedeutung, wengleich dort auch oft sensible Daten von Dritten Personen veröffentlicht werden, deren ausdrückliche Zustimmung⁶³¹ nicht vorliegt.

Daten in nur indirekt personenbezogener Form verletzen entsprechend § 8 Abs 2 DSGVO keine schutzwürdigen Geheimhaltungsinteressen.⁶³²

Für den Bereich der Verwendung von Daten im Finanzdienstleistungsbereich können die Ziffern 5⁶³³, 7⁶³⁴, 8⁶³⁵, 9⁶³⁶, 10⁶³⁷, 11⁶³⁸, 12⁶³⁹ und 13⁶⁴⁰ grundsätzlich in der rechtlichen Betrachtung vernachlässigt werden.

Gem § 9 Z 3 DSGVO werden schutzwürdige Geheimhaltungsinteressen dann nicht verletzt, wenn sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen.

Für den Bereich der Datenverwendung im öffentlichen Sektor verletzt nach § 9 Z 4 DSGVO die Verwendung durch Auftraggeber des öffentlichen Bereichs zur Erfüllung ihrer Verpflichtung zur Amtshilfe keine schutzwürdigen Geheimhaltungsinteressen.

Nach diesen beiden Bestimmungen sind daher entweder gesetzliche Vorschriften notwendig, die der Wahrung eines wichtigen öffentlichen Interesses dienen (Z 3) oder Auftraggeber des öffentlichen Bereichs, die ihre Verpflichtung zur Amtshilfe erfüllen. Das noch detailliert zu besprechende SWIFT-Abkommen⁶⁴¹ könnte hinsichtlich der datenschutzrechtlichen Recht-

⁶²⁸ „ausschließlich dann“ – vgl § 9, 1. Satz DSGVO.

⁶²⁹ Der Betroffene hat die Daten offenkundig selbst öffentlich gemacht.

⁶³⁰ Genannt seien etwa <http://www.twitter.com> und <http://www.facebook.com> (Stand: 18.08.2013).

⁶³¹ § 9 Z 6 DSGVO.

⁶³² Vgl § 9 Z 2 DSGVO.

⁶³³ Daten, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben.

⁶³⁴ Die Verarbeitung oder Übermittlung erfolgt zur Wahrung lebenswichtiger Interessen des Betroffenen und seine Zustimmung kann nicht rechtzeitig eingeholt werden.

⁶³⁵ Die Verwendung der Daten ist zur Wahrung lebenswichtiger Interessen eines anderen notwendig.

⁶³⁶ Verwendung von Daten ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig, wobei die Daten rechtmäßig ermittelt wurden.

⁶³⁷ § 45 (private Zwecke), § 46 (wissenschaftliche Forschung), § 47 (Benachrichtigung oder Befragung des Betroffenen) oder § 48a DSGVO (Katastrophenfall) werden erfüllt.

⁶³⁸ Verwendung ist erforderlich, um den Rechten und Pflichten des Arbeitgebers nachzukommen und nach besonderen Vorschriften zulässig.

⁶³⁹ Speziell geregelte Verwendung von Gesundheitsdaten.

⁶⁴⁰ Sonderregelung für nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck.

⁶⁴¹ Vgl V.B.6 SWIFT-Abkommen.

fertigung bei sensiblen Daten auf dieser Grundlage beruhen. Bei nicht-sensiblen Daten könnten analog § 8 Abs 1 Z 1 DSG (ausdrückliche gesetzliche Ermächtigung) bzw § 8 Abs 1 Z 4 iVm § 8 Abs 3 Z 1 und 2 DSG (wesentliche Voraussetzung für Auftraggeber des öffentlichen Bereichs für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe; durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe) als datenschutzrechtliche Rechtfertigungsgründe herangezogen werden. Die gesetzliche Regelung räumt somit dem öffentlichen Bereich beim Bestehen von Gesetzen oder einer Verpflichtung zur Amtshilfe sehr weitreichende Rechtfertigungsgründe ein. Umso wichtiger ist die grundrechtliche Prüfung einzelner Materiengesetze, damit auch materiell betrachtet keine schutzwürdigen Geheimhaltungsinteressen verletzt werden.

Der für die Errichtung von Informationsverbundsystemen und va bankinternen Datenanwendungen bedeutsamste Rechtfertigungsgrund stellt wohl § 9 Z 6 DSG dar. In Umsetzung des Art 8 Abs 2 lit a der RL 1995/46/EG wurde ebenfalls eine ausdrückliche Zustimmung für die Verwendung von sensiblen Daten vorgesehen. Diese muss nicht unbedingt schriftlich erteilt werden, wobei dies jedoch empfohlen wird.⁶⁴²

Hierbei wird in der Judikatur besonderer Wert auf die konkrete Formulierung der Zustimmungserklärung gelegt.⁶⁴³ Auf die mangels ausreichender Konkretisierung erfolgte Unwirksamklärung von einzelnen AGB-Bestimmungen bin ich bereits weiter oben eingegangen.⁶⁴⁴

Ad 3) Erforderliches Ausmaß und gelindeste Mittel zum Eingriff in das Grundrecht:

Neben den bereits genannten Voraussetzungen (Berechtigung des Auftraggebers und keine Verletzung von schutzwürdigen Geheimhaltungsinteressen des Betroffenen) ist gem § 7 Abs 3 DSG für die Zulässigkeit einer Datenverwendung erforderlich, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 DSG eingehalten werden.⁶⁴⁵

⁶⁴² Pollirer/Weiss/Knyrim, DSG (2010) § 9 Anm 7.

⁶⁴³ Vgl OGH 19.11.2002, 4 Ob 179/02f; hilfreiche Vorschläge zur Gestaltung von Zustimmungserklärungen bieten Riegler/Trappitsch, Datenübermittlung und Zustimmungssproblematik im Datenschutzgesetz, RdW 2005, 341 (342 ff).

⁶⁴⁴ Vgl IV.F Exkurs: Bank AGB 2000 – mehrere Klauseln unwirksam.

⁶⁴⁵ Auf die Grundsätze des § 6 DSG werde ich im folgenden Punkt „Ad 4) Grundsätze des § 6 DSG“ eingehen.

Durch diese Bestimmung wird § 1 Abs 2 dritter Satz DSGVO⁶⁴⁶ einfachgesetzlich ausformuliert. Es handelt sich hierbei um eine besondere Ausprägung des Verhältnismäßigkeitsgebotes.⁶⁴⁷ Während das „herkömmliche“ Verhältnismäßigkeitsgebot die Eignung, Erforderlichkeit und Proportionalität des Eingriffs⁶⁴⁸ verlangt, ist nach dem Gebot des gelindesten Mittels unter den im engeren Sinn verhältnismäßigen Eingriffen nur der schonendste Eingriff zulässig.⁶⁴⁹

Ad 4) Grundsätze des § 6 DSGVO:

Jedenfalls müssen bei der Verarbeitung von Daten die Grundsätze des § 6 DSGVO eingehalten werden. Diese sind in § 6 Abs 1 Z 1 bis 5 DSGVO aufgezählt und lauten:

- Treu und Glauben und Rechtmäßigkeit,⁶⁵⁰
- strenge Zweckbindung,⁶⁵¹
- Beschränkung des Datenumfanges,⁶⁵²
- sachliche Richtigkeit und am neuesten Stand⁶⁵³ sowie
- begrenzte Aufbewahrungsdauer.⁶⁵⁴

Im Folgenden werde ich kurz auf die genannten Grundsätze eingehen. Zur tieferen Auseinandersetzung sei vor allem *Jahnel*⁶⁵⁵ empfohlen, der auch jeweils aktuelle Judikate zu den einzelnen Grundsätzen in seine Erörterung einbaut. Diese fünf Grundsätze finden sich bereits in Art 5 der Datenschutzkonvention des Europarates⁶⁵⁶ aus dem Jahr 1981, welche 1985 in Kraft trat.

Treu und Glauben und Rechtmäßigkeit:

⁶⁴⁶ „Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.“

⁶⁴⁷ *Jahnel*, Handbuch Datenschutzrecht, 2/67.

⁶⁴⁸ Die „Proportionalität des Eingriffs“ wird auch als Verhältnismäßigkeit im engeren Sinn bezeichnet.

⁶⁴⁹ Vgl. *Jahnel*, Handbuch Datenschutzrecht, 2/67 mit Verweis auf *Öhlinger*, Verfassungsrecht⁸ Rz 715 ff. *Walter/Mayer/Kucsko-Stadlmayer* sehen darin eine weitere Betonung des Grundsatzes der Verhältnismäßigkeit (*Walter/Mayer/Kucsko-Stadlmayer*, Verfassungsrecht¹⁰ Rz 1444, S 712 f).

⁶⁵⁰ § 6 Abs 1 Z 1 DSGVO.

⁶⁵¹ § 6 Abs 1 Z 2 und 3 DSGVO.

⁶⁵² § 6 Abs 1 Z 3 DSGVO.

⁶⁵³ § 6 Abs 1 Z 4 DSGVO.

⁶⁵⁴ § 6 Abs 1 Z 5 DSGVO.

⁶⁵⁵ *Jahnel*, Handbuch Datenschutzrecht, 4/98 bis 4/118.

⁶⁵⁶ Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr 108) – vgl. auch <http://conventions.coe.int/treaty/ger/treaties/html/108.htm>.

Einen Aspekt davon habe ich bereits weiter oben angesprochen.⁶⁵⁷ Zu erwähnen ist, dass gem § 6 Abs 4 DSG für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten können, um festzulegen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist. Diese Verhaltensregeln dürfen gem § 6 Abs 4 zweiter Satz DSG nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

Strenge Zweckbindung:

Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden, wobei Ausnahmen für wissenschaftliche und statistische Zwecke nach Maßgabe der §§ 46 und 47 DSG möglich sind. Der Zweck einer Datenverwendung muss daher von vornherein festgelegt werden.

Beschränkung des Datenumfanges:

Daten dürfen nur verwendet werden, soweit sie für den Zweck einer Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen. So kann etwa auch innerhalb eines Unternehmens eine widerrechtliche Verwendung von Daten vorliegen, wenn zB Kundendaten, die zur Bearbeitung von Buchbestellungen verarbeitet wurden, plötzlich für Marketing-Zwecke verwendet werden.

Sachliche Richtigkeit und am neuesten Stand:

„Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.“⁶⁵⁸ Durch eine regelmäßige Überprüfung auf Aktualität sollen ungerechtfertigte Nachteile für Betroffene vermieden werden.⁶⁵⁹

Begrenzte Aufbewahrungsdauer:

Die Aufbewahrung von Daten in personenbezogener Form ist nur solange erlaubt, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Aus besonderen

⁶⁵⁷ Vgl IV.C.4 Judikatur der österr DSK.

⁶⁵⁸ § 6 Abs 1 Z 4 DSG.

⁶⁵⁹ Vgl Pollirer/Weiss/Knyrim, DSG (2010) § 6 ErläutRV, Zu Abs 1, S 38 f.

gesetzlichen, insbesondere archivrechtlichen Vorschriften, kann sich aber eine längere Aufbewahrungsdauer ergeben.⁶⁶⁰

c) Übermittlung

Eine Übermittlung liegt, wie bereits ausführlich erläutert, vor, wenn Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister weiter gegeben werden. Davon werden insbesondere auch die Veröffentlichung von Daten, sowie die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers erfasst.

Aus der gesetzlichen Definition⁶⁶¹ wurden in der Literatur drei unterschiedliche Formen der Übermittlung herausdifferenziert, die ich kurz wiedergeben werde, ohne auf diese näher einzugehen.⁶⁶²

- 1) Weitergabe von Daten an Dritte außer Betroffener, Auftraggeber oder Dienstleister,
- 2) Veröffentlichung von Daten,
- 3) Verwendung von Daten für ein anderes Gebiet des Auftraggebers.

Bei der Übermittlung von Daten ist im Vergleich zur Verarbeitung *eine wesentliche zusätzliche Voraussetzung* zu erfüllen: Der Empfänger muss dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht haben.

Die Vorschriften, welche für die Zulässigkeit einer Datenverwendung gelten, gelten für die Verarbeitung und Übermittlung von Daten gleichermaßen, weil die Verwendung von Daten nach der Begriffsdefinition⁶⁶³ sowohl die Verarbeitung, als auch die Übermittlung von Daten umfasst.

Vor der DSGVO-Novelle 2010 fand sich in § 4 Z 12 DSGVO – ebenso wie in § 4 Z 8 DSGVO – eine Bezugnahme auf „Daten einer Datenanwendung“. Es muss sich somit nach geltender Rechtslage nicht mehr um Daten einer Datenanwendung handeln, wodurch schlicht der Begriff „Daten“ im Gesetzestext zu finden ist. Dies stellt eine Erweiterung des

⁶⁶⁰ § 6 Abs 1 Z 5 DSGVO.

⁶⁶¹ § 4 Z 12 DSGVO.

⁶⁶² Vgl zum tieferen Verständnis *Jahnel*, Handbuch Datenschutzrecht, 3/116 bis 3/126 und *Dörfler/Siegwart* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 519 f.

⁶⁶³ Vgl § 4 Z 8 DSGVO.

Anwendungsbereiches dar, die vereinzelt in der Literatur auch nach Inkrafttreten der DSGVO-Novelle 2010 noch nicht überall eingearbeitet wurde.⁶⁶⁴

d) Überlassung

Eine Überlassung liegt gem § 4 Z 11 DSGVO vor, wenn Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses weitergegeben werden. Es handelt sich somit bei Weitergabe von Daten zwischen Auftraggeber und Dienstleister nicht um eine Übermittlung im datenschutzrechtlichen Sinn.

Vor der DSGVO-Novelle 2010 definierte § 4 Z 11 DSGVO, dass eine Überlassung vorliegt, wenn Daten vom Auftraggeber an einen Dienstleister weitergegeben werden. Durch die Verwendung des Wortes „zwischen“ ist klargestellt, dass eine Überlassung auch vorliegt, wenn Daten vom Dienstleister an den Auftraggeber weitergegeben werden.⁶⁶⁵

Nachdem nun Klarheit über die begrifflichen Definitionen herrscht, werde ich auf innereuropäische⁶⁶⁶ und internationale Vorgänge der Datenverarbeitung, -übermittlung und -überlassung eingehen und Anleitungen dazu geben, wann diese Vorgänge rechtlich zulässig sind bzw wonach die Rechtmäßigkeit zu beurteilen ist. Die Zulässigkeit der Datenverarbeitung, -übermittlung und -überlassung in Österreich dürfte ausreichend erörtert worden sein.

4. Datenübermittlung und -überlassung in MS des EWR

a) Allgemeines

Die Datenschutzrichtlinie gibt in manchen Bereichen eine andere Terminologie vor. So entspricht der Begriff „Verarbeiten“ der Datenschutzrichtlinie dem Begriff „Verwenden“ im österr DSGVO.⁶⁶⁷ Inwiefern diese Begriffsunterscheidung zum Verständnis des Rechtsanwenders

⁶⁶⁴ Vgl *Pollirer/Weiss/Knyrim*, DSGVO (2010) § 4 Anm 12, wo noch auf die Daten aus einer Datenanwendung Bezug genommen wird, wenngleich sich unter *Pollirer/Weiss/Knyrim*, DSGVO (2010) § 4 ErläutRV 2010, Zu Z 8 und 12 der Hinweis auf die Streichung der Bezugnahme auf „Datenanwendung“ findet.

⁶⁶⁵ Vgl *Jahnel*, Handbuch Datenschutzrecht, 3/128.

⁶⁶⁶ Unterschieden wird hier nach Mitgliedstaaten des EWR und Nichtmitgliedstaaten des EWR.

⁶⁶⁷ Vgl Überschrift der Datenschutzrichtlinie (RL zum Schutz natürlicher Personen bei der *Verarbeitung* personenbezogener Daten und zum freien Datenverkehr) sowie Art 2 lit b der RL 1995/46/EG (*Verarbeitung*: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die *Weitergabe durch Übermittlung*, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten) und § 4 Z 8 und 9 österr DSGVO, woraus hervorgeht, dass die Übermittlung im österr Recht nicht vom Begriff der Verarbeitung erfasst ist; vgl auch bereits II.A.2.b) Verwendung von Daten.

beitragen soll, kann von mir nicht erschlossen werden. Um eine einheitliche Auslegung zu gewährleisten, wäre auch die Verwendung einheitlicher Begrifflichkeiten bei der Umsetzung von Richtlinienbestimmungen sinnvoll.⁶⁶⁸

Im Folgenden werde ich die Datenübermittlung und Datenüberlassung in Mitgliedstaaten des EWR besprechen. Die Zulässigkeit der Datenverwendung im jeweiligen Mitgliedstaat ist nach den Bestimmungen der RL 1995/46/EG und den nationalen Gesetzen zu beurteilen. In diesem Abschnitt geht es somit um die Frage, wann ein Datentransfer zulässig ist.

Die zentrale österr Regelung für den Datentransfer innerhalb der Europäischen Union bzw des Europäischen Wirtschaftsraumes ist § 12 DSG. Darin wird die genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland geregelt.

Durch die DSG-Novelle 2010 wurde in § 12 Abs 1 erster Satz DSG klargestellt, dass eine genehmigungsfreie Übermittlung und Überlassung nicht nur in die Mitgliedstaaten der Europäischen Union, sondern auch in alle Mitgliedstaaten des Europäischen Wirtschaftsraums erfolgen kann. Somit wurden zusätzlich zu den Staaten der Europäischen Union die Staaten Island, Liechtenstein und Norwegen erfasst.

Genehmigungspflichtig ist jedoch auch im Europäischen Wirtschaftsraum der Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.⁶⁶⁹

Wann ein Datentransfer in Nicht-Mitgliedstaaten des EWR („Drittstaaten“) zulässig ist, werde ich im nächsten Abschnitt des Kapitels erörtern.

b) Verwendung

Ob die Verwendung der Daten im jeweiligen EWR-Mitgliedstaat rechtmäßig erfolgt, ist anhand der nationalen Bestimmungen, welche in Einklang mit der RL 1995/46/EG sein müssen, zu prüfen. Durch einen Beschluss des Gemeinsamen EWR-Ausschusses⁶⁷⁰ wurde der räumliche Anwendungsbereich der Datenschutz-RL von den Mitgliedstaaten der Europäischen Union auf alle EWR-Mitgliedstaaten erweitert. Somit hatten auch Island,

⁶⁶⁸ Zur uneinheitlichen Steuerhinterziehungs- und Missbrauchtsterminologie im europäischen Steuerrecht und die allgemein zu beachtenden Leitlinien für die redaktionelle Qualität der gemeinschaftlichen Rechtsakte: *Bergmann*, Steuerhinterziehungs- und Missbrauchsterminologie im europäischen Steuerrecht, SWI 2010, 477 (481, FN 43).

⁶⁶⁹ Vgl § 12 Abs 1 letzter Satz DSG.

⁶⁷⁰ Beschluss des Gemeinsamen EWR-Ausschusses Nr 83/1999 vom 25. Juni 1999 zur Änderung des Protokolls 37 und des Anhangs IX (Telekommunikationsdienste) zum EWR-Abkommen (=ABl L 296 vom 23.11.2000, S 41-43).

Liechtenstein und Norwegen die Datenschutz-Richtlinie als Teil des „Acquis Communautaire“ in innerstaatliches Recht umzusetzen.

Voraussetzung für die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung⁶⁷¹ sind oder nach der Übermittlung sein sollen, in andere Staaten ist, dass in diesem Staat ein angemessenes Datenschutzniveau besteht.⁶⁷² Auch hat die Datenanwendung in Österreich rechtmäßig iSd § 7 DSGVO zu sein, damit eine Übermittlung oder Überlassung in das Ausland möglich ist.⁶⁷³

c) Übermittlung und Überlassung

Gem § 12 Abs 1 DSGVO ist die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes nicht genehmigungspflichtig iSd § 13 DSGVO.

Voraussetzung für die Übermittlung ist, wie bereits erwähnt, dass die Datenanwendung in Österreich rechtmäßig nach § 7 DSGVO ist.

Bei Überlassungen ins Ausland muss darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber bzw bei Überlassung an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich⁶⁷⁴ an den inländischen Dienstleister vorliegen, dass der ausländische Dienstleister die Dienstleistungspflichten gem § 11 Abs 1 DSGVO einhalten werde. Dies ist nicht erforderlich, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.⁶⁷⁵

5. Datenübermittlung und -überlassung in „Drittstaaten“

a) Allgemeines

Als „Drittstaat“ iSd österr DSGVO werden die Nicht-Mitgliedstaaten des EWR verstanden. Diese sind nicht zur Umsetzung der RL 1995/46/EG verpflichtet, weshalb jeweils im Einzelfall zu überprüfen ist, ob in diesem Drittstaat ein angemessenes Datenschutzniveau besteht oder eine

⁶⁷¹ Dies entspricht der „Verwendung“ iSd österr DSGVO, vgl V.A.4.a) Allgemeines.

⁶⁷² Vgl Art 25 Abs 1 der RL 1995/46/EG.

⁶⁷³ § 12 Abs 5 erster Satz DSGVO.

⁶⁷⁴ Vgl § 13 Abs 5 DSGVO.

⁶⁷⁵ Vgl § 12 Abs 5 zweiter und dritter Satz.

Ausnahmeregelung des § 12 Abs 3 oder 4⁶⁷⁶ DSG vorliegt. Wenn kein angemessenes Datenschutzniveau besteht und auch keine Ausnahme nach § 12 Abs 3 oder 4 DSG vorliegt, hat die DSK die Übermittlung und Überlassung von Daten ins Ausland in einem Genehmigungsverfahren zu überprüfen.⁶⁷⁷ Die Genehmigung kann auch an die Erfüllung von Bedingungen und Auflagen gebunden werden.⁶⁷⁸

Um einen Überblick über die Ausnahmebestimmungen in § 12 Abs 3 und 4 DSG zu erhalten, werde ich einen tabellarischen Vergleich anstellen. Vorweg sei erwähnt, dass Art 26 Abs 1 der RL 1995/46/EG andere innerstaatliche Regelungen zulässt.⁶⁷⁹

<i>Österr Bestimmung</i>	<i>Richtlinienbestimmung</i>	<i>Thema</i>	<i>Vergleich zur RL</i>
§ 12 Abs 3 Z 1	Art 26 Abs 1 lit f)	Zulässige Veröffentlichung im Inland	In RL: Bezugnahme auf Register
§ 12 Abs 3 Z 2	Art 26 Abs 1 erster Satz	Indirekt personenbezogene Daten	Österr Ausnahme
§ 12 Abs 3 Z 3	Art 26 Abs 1 erster Satz	Innerstaatliches Gesetz sieht Übermittlung oder Überlassung vor	Österr Ausnahme
§ 12 Abs 3 Z 4	Art 26 Abs 1 erster Satz	Private Zwecke (§ 45) oder publizistische Tätigkeit (§ 48)	Österr Ausnahme
§ 12 Abs 3 Z 5	Art 26 Abs 1 lit a)	Zustimmung ohne jeden Zweifel	Vgl RL!
§ 12 Abs 3 Z 6	Art 26 Abs 1 lit c)	Übermittlung als Wesensgrundlage eines (auch zw AG + Drittem)	Vgl RL!

⁶⁷⁶ Nach § 12 Abs 3 DSG ist der Datenverkehr ins Ausland beim Erfüllen einer der insgesamt zehn Ziffern genehmigungsfrei. Bei § 12 Abs 4 DSG kann die Genehmigung der DSK nicht rechtzeitig eingeholt werden, die DSK ist jedoch umgehend zu informieren.

⁶⁷⁷ § 13 Abs 1 DSG.

⁶⁷⁸ § 13 Abs 1 zweiter Satz DSG.

⁶⁷⁹ Vgl „vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht“ (Art 26 Abs 1 erster Satz).

		abgeschlossenen Vertrages	
§ 12 Abs 3 Z 7	Art 26 Abs 1 lit d)	Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden	Vgl RL!
§ 12 Abs 3 Z 8	Art 26 Abs 1 erster Satz	In StandardVO (§ 17 Abs 2 Z 6) oder MusterVO (§ 19 Abs 2) ausdrücklich angeführt	Österr Ausnahme
§ 12 Abs 3 Z 9	Art 26 Abs 1 erster Satz	Datenverkehr mit österr Dienststellen im Ausland	Österr Ausnahme
§ 12 Abs 3 Z 10	Art 26 Abs 1 erster Satz	Datenanwendungen, die gem § 17 Abs 3 von der Meldepflicht ausgenommen sind	Österr Ausnahme
§ 12 Abs 4 Z 1	Art 26 Abs 1 lit d)	Wichtiges öffentliches Interesse	In Ö: nur bei Dringlichkeit + Mitteilungspflicht an DSK!
§ 12 Abs 4 Z 2	Art 26 Abs 1 lit e)	Lebenswichtige Interessen des Betroffenen	In Ö: nur bei Dringlichkeit + Mitteilungspflicht an DSK!
-	Art 26 Abs 1 lit b)	Übermittlung zur Durchführung von vorvertraglichen Maßnahmen auf Antrag des Betroffenen erforderlich	Aspekt der vorvertraglichen Maßnahmen in Art 26 Abs 1 lit b) findet sich idZ nicht im DSG!

b) Angemessenes Datenschutzniveau

Leitlinien zur Feststellung der Angemessenheit:

Gem Art 25 Abs 2 der RL 1995/46/EG wird die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. So sind insbesondere die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen zu berücksichtigen.

§ 12 Abs 2 DSG sieht die Ausgestaltung der Grundsätze des § 6 Abs 1 DSG in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung als maßgebend an.⁶⁸⁰

Feststellung der Angemessenheit:

Gem Art 25 Abs 6 kann die Europäische Kommission nach dem Verfahren des Art 31 Abs 2⁶⁸¹ feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Abs 5 leg cit eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau nach Art 25 Abs 2 gewährleistet. Gem zweiter Satz leg cit haben die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen zu treffen.

In § 12 Abs 2 zweiter Satz DSG wird normiert, dass unter Beachtung des § 55 Z 1 DSG⁶⁸² der Bundeskanzler durch Verordnung feststellen kann, welche Drittstaaten angemessenen Datenschutz gewährleisten.

Die europarechtliche Verpflichtung zur Kundmachung jener Staaten, für die in einem Verfahren gem Art 31 Abs 2 der RL 1995/46/EG festgestellt wurde, dass sie ein angemessenes Datenschutzniveau erfüllen, wurde somit auch im österr DSG normiert.

⁶⁸⁰ § 12 Abs 2 dritter Satz DSG.

⁶⁸¹ Sog „Ausschussverfahren“.

⁶⁸² Demnach ist der Inhalt der in einem Verfahren gem Art 31 Abs 2 der RL 1995/46/ getroffenen Feststellungen der EK über das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland vom Bundeskanzler im BGBl kundzumachen. Gem § 55 Z 2 ist auch die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland im BGBl kundzumachen.

Welche Staaten ein angemessenes Schutzniveau erfüllen, wurde durch die Datenschutzangemessenheitsverordnung⁶⁸³ kundgemacht. Diese umfasste in § 1 DSAV mit Stand Mai 2013 die Staaten Schweiz und Ungarn.

Dadurch, dass Ungarn seit 01.05.2004 Mitglied der Europäischen Union ist, ist die Übermittlung und Überlassung von Daten keinen Beschränkungen im Sinne des § 13 DSG unterworfen.⁶⁸⁴ Es wird daher von der Angemessenheit des Datenschutzniveaus ausgegangen, da Ungarn verpflichtet wurde, gemeinschaftsrechtliche Bestimmungen umzusetzen. Die Nennung Ungarns in § 1 DSAV war somit nicht mehr notwendig.

Unter den bibliographischen Angaben im Unterpunkt „Verbindungen zwischen Dokumenten“ sind auf der Rechtsinformationswebseite der Europäischen Union⁶⁸⁵ zur RL 1995/46/EG jene Dokumente zu finden, für die dieser Rechtsakt Rechtsgrundlage ist. Bei weiterer Sortierung nach „Celex-Sektor“ kann die Einschränkung auf das aus der RL 1995/46/EG abgeleitete Recht gewählt werden. Hierbei finden sich zahlreiche Beschlüsse der Kommission, mit denen die Angemessenheit des Datenschutzniveaus in Drittstaaten festgestellt wurde. Das Datenschutzniveau folgender Staaten wurde als angemessen festgestellt: Neuseeland⁶⁸⁶, Republik Östlich des Uruguay⁶⁸⁷, Israel⁶⁸⁸ (hinsichtlich Uruguay und Israel wurde die Angemessenheit jedoch nur auf den Bereich der automatisierten Verarbeitung personenbezogener Daten beschränkt), Andorra⁶⁸⁹, Färöer⁶⁹⁰, Jersey⁶⁹¹, Isle of Man⁶⁹²,

⁶⁸³ BGBl II Nr 521/1999 idF BGBl II Nr 213/2013: Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV).

⁶⁸⁴ § 12 Abs 1 DSG; vgl auch weiter oben V.A.4.c) Übermittlung und Überlassung.

⁶⁸⁵ <http://www.eur-lex.europa.eu> (Stand: 18.08.2013).

⁶⁸⁶ 2013/65/EU: Durchführungsbeschluss der Kommission vom 19. Dezember 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Neuseeland (ABl L 28 vom 30.1.2013, S 12–14).

⁶⁸⁷ 2012/484/EU: Durchführungsbeschluss der Kommission vom 21. August 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in der Republik Östlich des Uruguay im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (ABl L 227 vom 23.8.2012, S 11–14).

⁶⁸⁸ 2011/61/EU: Beschluss der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (= ABl L 27 vom 1.2.2011, S 39-42).

⁶⁸⁹ 2010/625/EU: Beschluss der Kommission vom 19. Oktober 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Andorra (= ABl L 277 vom 21.10.2010, S 27-29).

⁶⁹⁰ 2010/146/EU: Beschluss der Kommission vom 5. März 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus, den das färöische Gesetz über die Verarbeitung personenbezogener Daten bietet (= ABl L 58 vom 9.3.2010, S 17-19).

⁶⁹¹ 2008/393/EG: Entscheidung der Kommission vom 8. Mai 2008 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Jersey (= ABl L 138 vom 28.5.2008, S 21-23).

Guernsey⁶⁹³, Argentinien⁶⁹⁴, Kanada⁶⁹⁵ (hierbei ist jedoch zu prüfen, ob der jeweilige Empfänger unter den Personal Information Protection und Electronic Documents Act – das kanadische Datenschutzgesetz – fällt), Ungarn⁶⁹⁶ (mittlerweile nicht mehr notwendig) und Schweiz⁶⁹⁷.

Die mittlerweile deutlich erweiterte Liste der Staaten mit angemessenem Datenschutzniveau wurde in Österreich erst durch die DSAV-Novelle 2013 umgesetzt. Um den gemeinschaftsrechtlichen Verpflichtungen, welche sich auch im österr DSG finden⁶⁹⁸, nachzukommen und auch um die Transparenz und Klarheit der Regelung zu fördern, war die DSAV unbedingt entsprechend abzuändern. Der dadurch entstehende Mehraufwand war sehr überschaubar und wurde sehr lange (über zehn Jahre) nicht umgesetzt.

§ 1 DSAV normiert idF BGBl II Nr 213/2013, dass die Übermittlung und Überlassung von Daten aus Datenanwendungen an Empfänger in Staaten, die weder Mitgliedstaaten der Europäischen Union noch Vertragsparteien des EWR sind (Drittstaaten), keiner Genehmigung der DSK bedarf, wenn die Übermittlung oder Überlassung in einen der folgenden Drittstaaten oder in eines der folgenden, für die Zwecke dieser Verordnung als Drittstaaten geltenden Gebiete erfolgt: Schweiz, Argentinien, Guernsey, Insel Man, Jersey, Färöer Inseln, Andorra, Uruguay und Neuseeland.

Zusätzlich normiert § 1 Abs 2 DSAV, dass die Übermittlung und Überlassung von Daten aus Datenanwendungen an Empfänger in Drittstaaten dann keiner Genehmigung der DSK bedarf, wenn die Übermittlung oder Überlassung in einen der folgenden Staaten entsprechend den angeführten Voraussetzungen erfolgt:

⁶⁹² 2004/411/EG: Entscheidung der Kommission vom 28. April 2004 über die Angemessenheit des Schutzes personenbezogener Daten auf der Isle of Man (= ABl L 151 vom 30.4.2004, S 51-54).

⁶⁹³ 2003/821/EG: Entscheidung der Kommission vom 21. November 2003 über die Angemessenheit des Schutzes personenbezogener Daten in Guernsey (= ABl L 308 vom 25.11.2003, S 27-28).

⁶⁹⁴ 2003/490/EG: Entscheidung der Kommission vom 30. Juni 2003 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien (= ABl L 168 vom 5.7.2003, S 19-22).

⁶⁹⁵ 2002/2/EG: Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (= ABl L 2 vom 4.1.2002, S 13-16).

⁶⁹⁶ 2000/519/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in Ungarn (= ABl L 215 vom 25.8.2000, S 4-6).

⁶⁹⁷ 2000/518/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz (= ABl L 215 vom 25.8.2000, S 1-3).

⁶⁹⁸ Vgl § 12 Abs 2 zweiter Satz DSG.

1. *Vereinigte Staaten von Amerika, entsprechend der Entscheidung 2000/520/EG der Kommission gemäß der Richtlinie 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl Nr L 215 vom 25.8.2000, S 7, in der Fassung der Berichtigung ABl Nr L 115 vom 25.4.2001, S 14;*

2. *Kanada, entsprechend der Entscheidung 2002/2/EG der Kommission gemäß der Richtlinie 95/46/EG über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl Nr L 2 vom 4.1.2002, S 13;*

3. *Israel, entsprechend dem Beschluss 2011/61/EU der Kommission gemäß der Richtlinie 95/46/EG über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten, ABl Nr L 27 vom 1.2.2011, S 39.⁶⁹⁹*

In den einzelnen Entscheidungen und Beschlüssen⁷⁰⁰ der Europäischen Kommission wird jeweils festgehalten, dass die Mitgliedstaaten zur Umsetzung verpflichtet sind. Exemplarisch sei etwa nur auf Art 6 des Beschlusses 2010/625/EU⁷⁰¹ (hinsichtlich der Angemessenheit des Datenschutzniveaus in Andorra) verwiesen, der normiert, dass die Mitgliedstaaten bis 1. Januar 2011 die erforderlichen Maßnahmen zu ergreifen haben, um dem Beschluss nachzukommen. Ähnliche Fristsetzungen finden sich auch in den anderen Entscheidungen und Beschlüssen. Österreich hatte daher dringend die erforderlichen Maßnahmen zu ergreifen und die Liste der Staaten, die nach Ansicht der Europäischen Kommission über ein angemessenes Datenschutzniveau verfügen, in § 1 DSAV zu ergänzen.

⁶⁹⁹ Vgl § 1 Abs 2 der DSAV.

⁷⁰⁰ Bis zum Vertrag von Lissabon ergingen Beschlüsse der EK als „Entscheidung“; vgl Art 249 des EGV idF der konsolidierten Fassung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft (= ABl C 321E vom 29. Dezember 2006, S 1-331) und Art 288 AEUV idF der konsolidierten Fassung des Vertrags über die Arbeitsweise der Europäischen Union (= ABl C 83 vom 30. März 2010, S 47-200).

⁷⁰¹ Art 6 des Beschlusses 2010/625/EU vom 19. Oktober 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Andorra (= ABl L 277 vom 21.10.2010, S 27-29).

c) Übermittlung und Überlassung

Zur Zulässigkeit eines internationalen Datentransfers wurden bereits Checklisten erarbeitet.⁷⁰² Praktische Probleme ergeben sich vor allem bei Übermittlung von Kunden- oder Mitarbeiterdaten eines Konzerns aus verschiedenen EU-Mitgliedstaaten in ein und dieselbe Datenanwendung in einem Drittstaat, da dann die nationalen Umsetzungsbestimmungen zu beachten sind.⁷⁰³ Im Folgenden werde ich einen eigenen Überblick erarbeiten und dabei anhand der Angemessenheit des Datenschutzniveaus mehrere unterschiedliche Gruppen im Zusammenhang mit dem Datenverkehr in Drittstaaten bilden:

1) Angemessenheit wurde von EK im Verfahren nach Art 31 Abs 2 der RL festgestellt:

Wie bereits erwähnt, wurde für folgende Staaten die Angemessenheit des Datenschutzniveaus festgestellt: Israel (Angemessenheit nur hinsichtlich der automatisierten Verarbeitung von personenbezogenen Daten), Andorra, Färöer, Jersey, Isle of Man, Guernsey, Argentinien, Kanada (nur, wenn der jeweilige Empfänger unter den Personal Information Protection and Electronic Documents Act – das kanadische Datenschutzgesetz – fällt), Ungarn (seit 2004 EU-Mitgliedstaat, daher gilt § 12 Abs 1 DSG) und Schweiz.⁷⁰⁴

Die Europäische Kommission stellt die Angemessenheit nach dem Verfahren gem Art 31 Abs 2 der Datenschutzrichtlinie fest. Die erforderlichen Umsetzungen in Österreich sind bislang nur hinsichtlich Ungarn und Schweiz erfolgt.

Die im Verfahren nach Art 31 Abs 2 leg cit erlassenen Maßnahmen gelten nach Ansicht von *Jahnel* unmittelbar.⁷⁰⁵ *Jahnel* verweist auf die im Fall von nicht richtlinienkonformer Umsetzung zu ergreifenden Rechtsmöglichkeiten. *Knyrim* beschreibt im 2003 herausgegebenen Buch⁷⁰⁶ die Praxis der DSK, die entsprechend der mangelnden Umsetzung Österreichs weiterhin einen schriftlichen Antrag auf Genehmigung der Datenübermittlung nach § 13 DSG verlangt, soweit nicht die Ausnahmebestimmungen des § 12 DSG anwendbar sind. Dies sieht er aus österr Sicht als gesetzeskonform an, verweist aber auf Amts- oder

⁷⁰² Vgl etwa *Knyrim*, Zulässigkeit eines internationalen Datenverkehrs nach DSG 2000, *ecolex* 2002, 470.

⁷⁰³ *Knyrim*, Datenschutz brems Austausch in internationalen Konzernen, *DiePresse* 2006/44/01.

⁷⁰⁴ Vgl weiter oben V.A.5.b) Angemessenes Datenschutzniveau.

⁷⁰⁵ *Jahnel*, Handbuch Datenschutzrecht, 4/142 mit Verweis auf *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 13, Anm 12, 161 und aA *Knyrim*, Datenschutzrecht, 133 und 234.

⁷⁰⁶ Vgl *Knyrim*, Datenschutzrecht, 133.

Staatshaftungsansprüche, wenn die DSK im Widerspruch zur Kommissionsentscheidung die Datenübermittlung aus Zweifeln am Datenschutzniveau in Kanada nicht genehmigt.⁷⁰⁷

In der zweiten Auflage⁷⁰⁸ beschreibt er die sich seit 1999 entwickelte Praxis, die Entscheidung hinsichtlich der Adäquanz des datenschutzrechtlichen Niveaus von Drittstaaten der Europäischen Kommission zu überlassen.⁷⁰⁹

Auch ich kann mich der Meinung *Jahnels* insofern anschließen, als die im Fall von nicht richtlinienkonformer Umsetzung zu ergreifenden Rechtsmöglichkeiten auch diesfalls gelten. Eine ablehnende Haltung *Knyrims* erschließt sich aus der aktualisierten Auflage des Buches nicht mehr. Daher kann das nähere Besprechen der anderen Ansicht hier von mir vernachlässigt werden.

2) Angemessenheit wurde von Österreich nach Art 26 Abs 2 der RL festgestellt:

Der österr Bundeskanzler kann trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gem § 13 Abs 2 Z 1 DSG als gegeben feststellen.⁷¹⁰

An die Stelle der Verpflichtung zur Einholung einer Genehmigung tritt diesfalls die Pflicht zur Anzeige an die DSK, wobei diese binnen sechs Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen hat, wenn er keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder den Voraussetzungen nach § 12 Abs 5 DSG nicht entspricht. Wenn keine Untersagung mittels Bescheid erfolgt, ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

Diese österr Bestimmung beruht auf Art 26 Abs 2 der Datenschutz-RL. Nach Art 26 Abs 3 der RL hat Österreich auch die Europäische Kommission über die von ihr erteilten Genehmigungen zu unterrichten. Andere Mitgliedstaaten können einen in Bezug auf den Schutz der Privatsphäre, der Grundrechte und der Personen hinreichend begründeten Widerspruch einlegen, woraufhin die Europäische Kommission die geeigneten Maßnahmen wiederum nach dem Verfahren des Art 31 Abs 2 leg cit zu erlassen hat.

⁷⁰⁷ *Knyrim*, Datenschutzrecht, FN 289 auf S 133.

⁷⁰⁸ *Knyrim*, Datenschutzrecht².

⁷⁰⁹ *Knyrim*, Datenschutzrecht², 120 mwN.

⁷¹⁰ § 13 Abs 6 DSG.

3) Vereinigte Staaten Amerikas:

Mit den Vereinigten Staaten von Amerika wurde eine besondere datenschutzrechtliche Lösung gefunden, da dort keine umfassende Datenschutzgesetzgebung existiert. Abweichend vom europäischen Wirtschaftsraum besteht in den USA der regulatorische Ansatz in erster Linie in einer Selbstverpflichtung.⁷¹¹ In den USA wird Datenschutz zumeist als veräußerliche Ware gesehen, die dem Markt ausgesetzt ist („alienable commodity subject to the market“)⁷¹², wohingegen im kontinentaleuropäischen Bereich die Schutzfunktion des Staates betont wird.

Das zwischen der EU und den Vereinigten Staaten von Amerika abgeschlossene Abkommen, geht auf diesen Wesensunterschied ein und ermöglicht es amerikanischen Unternehmen, dem sog Safe Harbor („Sicherer Hafen“) beizutreten und dadurch die Safe Harbor Principles und die dazugehörigen – verbindlichen – Frequently Asked Questions (FAQ) zu beachten.⁷¹³ Auf das Abkommen werde ich an späterer Stelle noch detaillierter eingehen.⁷¹⁴

4) Sonderfälle:

Weiters ist bei der Prüfung, ob eine Datenübermittlung oder –überlassung rechtmäßig ist, zu beachten, ob nicht eine der folgenden besonderen Ausnahmen vorliegt:

Ausnahmen im Gesetz:

Das österr DSG nennt in Umsetzung der RL 1995/46/EG Ausnahmen, in denen der Datenverkehr ins Ausland genehmigungsfrei ist, wobei die Rechtmäßigkeit der Datenanwendung im Inland gegeben sein muss.

Auf diese Ausnahmen bin ich bereits weiter oben⁷¹⁵ eingegangen, weshalb ich an dieser Stelle nicht alle Ausnahmen wiederholen werde.

Standard- und Musterverordnung:

Diese Ausnahme wird in § 12 Abs 3 Z 8 DSG erwähnt. Aufgrund der Bedeutung in der Praxis werde ich darauf kurz separat eingehen: Der Bundeskanzler kann gem § 17 Abs 2 Z 6 DSG durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu

⁷¹¹ *Jahnel*, Handbuch Datenschutzrecht, 4/140.

⁷¹² *Kobrin*, The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance, S 8 (November 2002) = <http://knowledge.wharton.upenn.edu/papers/1080.pdf> (Stand: 18.08.2013)

⁷¹³ Vgl *Jahnel*, Handbuch Datenschutzrecht, 4/140.

⁷¹⁴ Vgl weiter unten V.B.6.d) Exkurs: Safe Harbor.

⁷¹⁵ Vgl V.A.5.a) Allgemeines.

Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist.⁷¹⁶ Ebenso kann der Bundeskanzler nach § 19 Abs 3 DSGVO durch Verordnung Musteranwendungen festlegen, wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen. Diesfalls erfolgt eine vereinfachte Meldung.

Der Bundeskanzler hat aufgrund dieser Ermächtigungsnormen die Standard- und Muster-Verordnung erlassen.⁷¹⁷

Standardvertragsklauseln:

Sofern für einen Staat die Angemessenheit des Datenschutzniveaus nicht generell festgestellt wurde, kann die Rechtmäßigkeit des Datenverkehrs durch die DSK durch Bescheid festgestellt werden.⁷¹⁸ Dies kann geschehen, wenn im konkreten Einzelfall angemessener Datenschutz besteht⁷¹⁹ oder auch wenn aufgrund vertraglicher Vereinbarungen bzw einseitiger Zusagen des Antragstellers sichergestellt wird, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden.⁷²⁰ Hierbei handelt es sich – ähnlich wie nach deutschem Recht – auch nach österr Recht um einen echten Vertrag zugunsten Dritter,⁷²¹ sofern dem Betroffenen, der nicht Vertragspartei ist, unmittelbare Rechte eingeräumt werden. In Common-Law-Rechtsordnungen steht der vertragliche Anspruch für gewöhnlich allein dem Gläubiger und nicht dem Dritten zu, wobei etwa nach US-amerikanischem Recht auch Dritte, die nicht Parteien eines Vertrages sind, Ansprüche aus diesem Vertrag als sogenannte „third party beneficiaries“ erwerben können.⁷²² Es empfiehlt sich daher bei Errichtung eines Vertrages zwischen Übermittler und Empfänger im Rahmen ihrer internationalprivatrechtlichen

⁷¹⁶ § 17 Abs 2 Z 6 DSGVO.

⁷¹⁷ BGBl II Nr 312/2004 idF BGBl II Nr 213/2013: Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004).

⁷¹⁸ Vgl § 13 Abs 1 DSGVO.

⁷¹⁹ § 13 Abs 2 Z 1 DSGVO.

⁷²⁰ § 13 Abs 2 Z 2 DSGVO.

⁷²¹ Ellger, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem Europäischen Datenschutzrecht, RabelsZ 1996, 738 (764).

⁷²² Ellger, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem Europäischen Datenschutzrecht, RabelsZ 1996, 738 (765 f).

Privatautonomie eine Rechtsordnung als Vertragsstatut zu wählen, die einen Vertrag zugunsten Dritter zulässt.⁷²³

Die Europäische Kommission kann nach dem Verfahren des Art 31 Abs 2 der RL 1995/46/EG feststellen, dass bestimmte Standardvertragsklauseln ausreichende datenschutzrechtliche Garantien bieten.⁷²⁴ Die Mitgliedstaaten haben die aufgrund der Feststellung der Europäischen Kommission gebotenen Maßnahmen zu treffen.

Die Verwendung dieser Standardvertragsklauseln hat den Zweck, dass die Datenschutzbehörden der Mitgliedstaaten diese, wenn sie vereinbart sind, als ausreichende Garantien anerkennen müssen.⁷²⁵ Bislang ergingen vier Entscheidungen der Kommission zu den Standardvertragsklauseln:

- Standardvertragsklauseln für die Übermittlung an Auftragsverarbeiter 2010/87/EU,⁷²⁶
- Standardvertragsklauseln für die Übermittlung zwischen für die Datenverarbeitung Verantwortlichen 2004/915/EG,⁷²⁷
- Standardvertragsklauseln für die Übermittlung an Auftragsverarbeiter 2002/16/EG⁷²⁸ und
- Standardvertragsklauseln für die Übermittlung zwischen für die Datenverarbeitung Verantwortlichen 2001/497/EG.⁷²⁹

Die Standardvertragsklauseln für die Übermittlung an Auftragsverarbeiter 2002/16/EG wurden durch Art 7 Abs 1 des Beschlusses der Kommission 2010/87/EU ab dem 15. Mai 2010 aufgehoben. Durch die Standardvertragsklauseln 2004 wurde lediglich die Entscheidung aus dem Jahr 2001 geändert, wodurch die anderen Bestimmungen der Entscheidung

⁷²³ Vgl *Ellger*, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem Europäischen Datenschutzrecht, *RabelsZ* 1996, 738 (766).

⁷²⁴ Vgl Art 26 Abs 4 der RL 1995/46/EG.

⁷²⁵ *Knyrim*, Datenübermittlung in Drittländer: Standardvertragsklauseln der Europäischen Kommission, *AnwBl* 2001, 634 (634).

⁷²⁶ 2010/87/EU: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (= *ABl L* 39 vom 12.2.2010, S 5-18).

⁷²⁷ 2004/915/EG: Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (= *ABl L* 385 vom 29.12.2004, S 74-84).

⁷²⁸ 2002/16/EG: Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (= *ABl L* 6 vom 10.1.2002, S 52-62).

⁷²⁹ 2001/497/EG: Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (= *ABl L* 181 vom 4.7.2001, S 19-31).

2001/497/EG weiterhin gelten.⁷³⁰ Die sich jeweils im Anhang befindlichen Standardvertragsklauseln in Form von Vertragsformblättern sind nebeneinander anwendbar, wobei jedoch jedes der beiden Standardvertragsklauselwerke für sich „geschlossen“ ist.⁷³¹

Bevor die Standardvertragsklauseln von den Vertragsparteien unterschrieben werden, ist eine eingehende Auseinandersetzung mit diesen notwendig, da sie auch ungewöhnliche Bestimmungen zB über die Drittbegünstigung der betroffenen Datensubjekte und die Haftung der Vertragsparteien enthalten.⁷³²

Die sich nach der DSGVO-Novelle 2010 in § 13 Abs 6 DSGVO⁷³³ wieder findende Bestimmung normiert, dass der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus durch Verordnung festzustellen hat, dass für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat im konkreten Einzelfall ein angemessener Datenschutz besteht. Statt der Verpflichtung der Einholung einer Genehmigung ist diesfalls nur die Pflicht zur Anzeige an die DSK zu beachten, wobei die DSK binnen sechs Wochen ab Anzeige den angezeigten Datenverkehr untersagen kann, andernfalls der Datenverkehr als zulässig erachtet wird. Da eine solche Verordnung hinsichtlich der Klauseln bislang nicht erlassen wurde, ist auch beim Abschluss von Standardvertragsklauseln die Einholung einer Genehmigung erforderlich.

In Anschluss an *Andréewitch/Steiner* ist eine reine Anzeigepflicht, statt der Genehmigungspflicht wünschenswert.⁷³⁴ Weshalb die Verwendung dieser Standardvertragsklauseln mit der Verwendung privat vereinbarter Vertragsklauseln beinahe gleich gestellt wird, ist nicht nachvollziehbar. Die Möglichkeit einer Untersagung binnen sechs Wochen im Anzeigeverfahren würde meiner Meinung nach weiterhin die Behandlung besonderer Einzelfälle ermöglichen und gleichzeitig die Verwendung dieser Standardvertragsklauseln weiter fördern, um möglichst rasche Rechtssicherheit der für die Datenverarbeitung Verantwortlichen zu erlangen.

⁷³⁰ Vgl Art 1 der Entscheidung 2004/915/EG.

⁷³¹ *Andréewitch/Steiner*, Internationaler Datentransfer: Neue „alternative“ Standardvertragsklauseln, RdW 2006, 81 (81) mit Verweis auf den 3. Erwägungsgrund der Entscheidung der Kommission 2004/915/EG.

⁷³² *Knyrim*, Neuerungen im Datenverkehr mit Drittländern, *ecolex* 2002, 466 (468).

⁷³³ Vgl zuvor § 13 Abs 7 DSGVO idF vor der DSGVO-Novelle 2010.

⁷³⁴ *Andréewitch/Steiner*, Internationaler Datentransfer: Neue „alternative“ Standardvertragsklauseln, RdW 2006, 81 (83).

5) Genehmigungspflichtige Übermittlung und Überlassung (§ 13 DSG):

Der Auftraggeber hat vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der DSK einzuholen, soweit der Datenverkehr mit dem Ausland nicht gem § 12 DSG genehmigungsfrei ist. Die Tatsache der Genehmigung scheint im Datenverarbeitungsregister der DSK auf und ist damit öffentlich, der Genehmigungsbescheid ist es nicht.⁷³⁵

Die Genehmigung kann erteilt werden, wenn der Datenverkehr im Einzelfall einem angemessenen Datenschutzniveau entspricht oder keine schutzwürdigen Geheimhaltungsinteressen verletzt werden, wobei Bedingungen und Auflagen zulässig sind. Die Übermittlung und Überlassung muss im Inland jedenfalls rechtmäßig nach § 12 Abs 5 DSG sein.

Durch die DSG-Novelle 2010 wurde in § 13 Abs 2 Z 2 DSG klargestellt, dass die schutzwürdigen Geheimhaltungsinteressen auch insbesondere durch vertragliche Zusicherungen des Empfängers sowie einseitige Zusagen des Antragstellers (§ 19 Abs 2 DSG) im Genehmigungsantrag über die näheren Umstände der Datenverwendung im Ausland gewahrt werden können. Einseitige Zusagen des Antragstellers werden für diesen mit der Registrierung durch die DSK verbindlich.

d) Sonderbestimmungen im Bereich Finanzdienstleistungen

Da die sog Standardanwendungen die in der Praxis mit Abstand wichtigste Ausnahme⁷³⁶ von der Meldepflicht betreffen, werde ich auf diese speziell unter dem Gesichtspunkt des Bereiches Finanzdienstleistungen (va in Drittländern) eingehen. Bei den in der Anlage 1 (Standardanwendungen) und Anlage 2 (Musteranwendungen) zur Standard- und Musterverordnung 2004 (StMV 2004) enthaltenen Empfängerkreisen, die mit einem Stern (*) gekennzeichnet sind, ist die Übermittlung und Überlassung auch in Drittstaaten ohne angemessenen Datenschutz (§ 12 Abs 2 DSG) zulässig. Mehrfach findet sich darin ein Stern beim Empfängerkreis „Banken zur Abwicklung des Zahlungsverkehrs“ oder anderen Institutionen aus dem Bereich der Finanzdienstleistungen. Folgende Standardanwendungen (SA) und Musteranwendungen (MA) ermöglichen die Übermittlung und Überlassung von

⁷³⁵ Pollirer/Weiss/Knyrim, DSG (2010) § 13 Anm 9; zum Datenverarbeitungsregister: Jahnelt, Datenschutzrecht in der Praxis, 35 ff.

⁷³⁶ Jahnelt, Handbuch Datenschutzrecht, 6/9.

aufgezählten Betroffenenkreisen an die genannten Empfängerkreise, auch wenn kein angemessenes Datenschutzniveau besteht:⁷³⁷

- SA001: Rechnungswesen und Logistik

1* Banken zur Abwicklung des Zahlungsverkehrs

6* Inkassounternehmen zur Schuldeneintreibung (ins Ausland daher nur, soweit die Schuld im Ausland eingetrieben werden muss);

7* Fremdfinanzierer wie Leasing- oder Factoringunternehmen und Zessionare, sofern die Lieferung oder Leistung auf diese Weise fremdfinanziert ist;

- SA003: Mitgliederverwaltung

1* Banken zum Zweck der Zahlungsabwicklung;

- SA004: Abgabenverwaltung der Gemeinden und Gemeindeverbände

1* Banken;

- SA005: Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts

1* Banken zur Abwicklung des Zahlungsverkehrs;

- SA016: Mitglieder- und Funktionärsdatenverwaltung der Wirtschaftskammerorganisation

6* Geld- und Kreditinstitute zur Abwicklung des Zahlungsverkehrs;

- SA018: Wirtschaftskammerorganisation: Betreuung von Mitgliedern, künftigen Mitgliedern und Interessenten im In- und Ausland

6* Angehörige rechtsberatender und unterstützender Berufe (zB Rechtsanwälte, Notare, Wirtschaftstreuhänder) sowie Zessionare, Factoringunternehmen, Inkassobüros, Versicherungen, Kreditauskunfteien, Gläubigerschutzverbände in ihrer Funktion als Gläubigervertreter;

7* Geld- und Kreditinstitute;

- SA033: Datenübermittlung im Konzern – C. Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzern

⁷³⁷ Vgl StMV idF BGBl II Nr 306/2012.

3* Banken zur Abwicklung des Zahlungsverkehrs.

- MA001: Personentransport- und Hotelreservierung

2* Banken zur Abwicklung des Zahlungsverkehrs;

In der Praxis müssen daher die im Betrieb bestehenden Datenanwendungen und Datenübermittlungen analysiert und mit den Standard- und Mustieranwendungen verglichen werden.⁷³⁸ Wenn ein Betrieb mehr Datenarten verarbeitet oder an andere Empfänger übermittelt als in den Standardanwendungen angeführt, besteht eine Meldepflicht an die DSK, sonst besteht keine Meldepflicht.⁷³⁹ Zu praktischen Problemen im Zusammenhang mit der Standard- und Musterverordnung sei *Knyrim/Haidinger* empfohlen.⁷⁴⁰ Diese befürworten, besonders bei dringlichen Genehmigungsverfahren, vor allem regelmäßigen persönlichen Kontakt zu den zuständigen Sachbearbeitern, damit allfällige Probleme möglichst rasch gelöst werden können.⁷⁴¹

Die Begrifflichkeiten der Verordnung sind mE in weiten Teilen nicht nachvollziehbar. So wird im Zusammenhang mit SA016 und SA018 von „Geld- und Kreditinstituten“ gesprochen, an den anderen Stellen wird auf „Banken“ als Empfängerkreis verwiesen. Dass hierbei auf die eingangs erwähnten unterschiedlichen Rechtsformen eingegangen wird, ist aus der Verordnung nicht herauszulesen. Vielmehr deutet die unscharfe verwendete Terminologie daraufhin, dass die Begriffe möglichst weit zu verstehen sind, und somit etwa auch Einzahlungsgeschäfte, die über Zahlungsinstitute oder E-Geld-Institute abgewickelt werden, hierunter fallen können. Eine diesbezügliche Klarstellung wäre wünschenswert. Die in der Verordnung genannten Empfängerkreise, die mit einem Stern gekennzeichnet sind, ermöglichen eine sehr weitreichende Übermittlung und Überlassung von Daten in Drittstaaten ohne angemessenes Datenschutzniveau. Die mehr als 100 A4-Seiten umfassende Verordnung nennt detailliert die zulässigen Datenarten, die an die genannten Empfängerkreise ausgetauscht werden dürfen. Details sind den Anlagen zur Standard- und Musterverordnung 2004 zu entnehmen, die zuletzt durch BGBl II Nr 213/2013 geändert wurden.

⁷³⁸ Vgl. *Knyrim/Haidinger*, Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis, RDV 2005, 208 (209).

⁷³⁹ *Knyrim/Haidinger*, Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis, RDV 2005, 208 (209).

⁷⁴⁰ *Knyrim/Haidinger*, Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis, RDV 2005, 208 (209 f).

⁷⁴¹ *Knyrim/Haidinger*, Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis, RDV 2005, 208 (210).

B. Im Finanzbereich relevante Bestimmungen

Im Folgenden werde ich lediglich auf die im Zusammenhang mit Datenschutz und Finanzdienstleistungen relevanten europarechtlichen Grundlagen kurz eingehen. Dies soll die Prüfung von Rechtsfragen in diesem Bereich erleichtern, wobei abhängig vom Sachverhalt auch andere hier nicht erwähnte Rechtsbereiche relevant sein können.⁷⁴² Bereits 1999 wurde festgehalten, dass rund 80 Prozent der im Banken- und Finanzbereich geltenden gesetzlichen Regelungen auf europäischer Ebene gesetzt werden und bei der nationalen Umsetzung von Richtlinien den Mitgliedstaaten in der Regel wenig Spielraum bleibe.⁷⁴³

1. Verbraucherkreditrichtlinie

Art 8 der Verbraucherkreditrichtlinie⁷⁴⁴ enthält ua die Verpflichtung zur Bewertung der Kreditwürdigkeit des Verbrauchers. Kreditgeber aus anderen Mitgliedstaaten müssen aufgrund des Diskriminierungsverbotes unter denselben Bedingungen Zugang zu solchen Datenbanken haben wie inländische Kreditgeber.⁷⁴⁵ Gem Art 9 Abs 4 VKr-RL gilt Art 9 leg cit „unbeschadet“ der Datenschutzrichtlinie. Die Verbraucherkreditrichtlinie wurde in Österreich im Verbraucherkreditgesetz⁷⁴⁶ umgesetzt. §§ 7 und 8 VKrG enthalten Regelungen zum Verhältnis zum Datenschutzgesetz: § 7 Abs 4 und § 8 VKrG schreiben vor, dass die Bestimmungen des DSG unberührt bleiben. Gem § 7 Abs 5 VKrG ist § 28 Abs 2 DSG in der jeweils geltenden Fassung auf bei der DSK registrierte Informationsverbundsysteme kreditgebender Institutionen zur Bonitätsbeurteilung, bei denen die Verwendung auf § 8 Abs 1 Z 2⁷⁴⁷ oder Z 4⁷⁴⁸ DSG beruht, nicht anzuwenden. Der Betroffene kann daher nicht deshalb ohne Begründung Widerspruch erheben, weil die Aufnahme in die öffentlich zugängliche Datenanwendung nicht gesetzlich angeordnet wurde.⁷⁴⁹

⁷⁴² Vgl etwa die von *Reimer* genannte Vielzahl von Rechtsakten auf Ebene des Europarechts: *Reimer* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) 550.

⁷⁴³ *Rabe*, Kreditwirtschaftlich wichtige Vorhaben der EU, Kreditwesen 1999, 1209 (1209).

⁷⁴⁴ RL 2008/48/EG vom 23. April 2008 des Europäischen Parlaments und des Rates über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (ABl L 133 vom 22.05.2008, S 66-92).

⁷⁴⁵ Art 9 der RL 2008/48/EG.

⁷⁴⁶ BGBl I Nr 28/2010: Bundesgesetz über Verbraucherkreditverträge und andere Formen der Kreditierung zu Gunsten von Verbrauchern (Verbraucherkreditgesetz – VKrG).

⁷⁴⁷ Zustimmung des Betroffenen zur Verwendung seiner Daten.

⁷⁴⁸ Überwiegende berechnete Interessen des Auftraggebers oder eines Dritten erfordern die Verwendung.

⁷⁴⁹ Vgl auch die Ausführungen in IV.D.3 Zulässigkeit.

2. Zahlungsdiensterichtlinie

Mit der Umsetzung der Zahlungsdiensterichtlinie⁷⁵⁰ soll ein EU-weit einheitlicher rechtlicher Rahmen für Zahlungsdienste geschaffen werden, was auch die nötige rechtliche Basis für SEPA⁷⁵¹ schafft.⁷⁵² Was das Überweisungsgeschäft, die Ausgabe und Verwaltung von Zahlungsmitteln, das Kreditgeschäft und das Finanztransfergeschäft betrifft, können durch die Zahlungsdiensterichtlinie in Österreich sowohl Kreditinstitute mit einer Konzession nach § 1 BWG, als auch Zahlungsinstitute inhaltlich gleiche Tätigkeiten durchführen.⁷⁵³

Für die Zwecke des 2. Hauptstückes des Zahlungsdienstegesetzes,⁷⁵⁴ welches aufgrund der Zahlungsdiensterichtlinie ergangen ist, haben Zahlungsinstitute alle relevanten Aufzeichnungen und Belege mindestens fünf Jahre aufzubewahren.⁷⁵⁵ Die Verwendung der für die Zwecke des 2. Hauptstückes verarbeiteten Daten ist für Zwecke der Verhütung, Ermittlung oder Feststellung von Betrugsfällen im Zahlungsverkehr nach Maßgabe des Datenschutzgesetzes und nach Maßgabe der gesetzlichen Zuständigkeiten zulässig. Auch an anderen Stellen wird auf Bestimmungen des DSG verwiesen.⁷⁵⁶

3. Geldwäschebestimmungen

Es existieren in diesem Bereich drei Richtlinien und eine Verordnung, wobei die 3. Geldwäsche-Richtlinie vom Oktober 2005 die teilweise überholten Bestimmungen der 2. Geldwäsche-Richtlinie aufgehoben hat und an die aktuellen 40 Empfehlungen der Financial Action Task Force on Money Laundering (FATF) zur Geldwäschebekämpfung und die 9 Sonderempfehlungen zur Bekämpfung der Terrorismusfinanzierung angepasst hat:⁷⁵⁷

- die erste Geldwäsche-Richtlinie (GW-RL),⁷⁵⁸
- die zweite Geldwäsche-Richtlinie (2. GW-RL)⁷⁵⁹ und

⁷⁵⁰ Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (= ABl L 319 vom 05.12.2007, S 1-36).

⁷⁵¹ Vgl V.C.2 SEPA – Single European Payment Area.

⁷⁵² Wagner/Eigner, Aufsichtsrechtliche Aspekte der Zahlungsdiensterichtlinie, ÖBA 2008, 633 (634).

⁷⁵³ Wagner/Eigner, Aufsichtsrechtliche Aspekte der Zahlungsdiensterichtlinie, ÖBA 2008, 633 (648).

⁷⁵⁴ BGBl I Nr 66/2009, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG).

⁷⁵⁵ Vgl § 18 ZaDiG.

⁷⁵⁶ Vgl etwa die Verpflichtung zu Datensicherheitsmaßnahmen gem § 14 DSG in § 19 Abs 3 Z 3 ZaDiG sowie § 61 ZaDiG.

⁷⁵⁷ <https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html> (Stand: 18.08.2013).

⁷⁵⁸ Richtlinie 91/308/EWG des Rates vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (= ABl L 166 vom 28.6.1991, S 77-82).

⁷⁵⁹ Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (= ABl L 309 vom 25.11.2005, S 15-36).

- die dritte Geldwäsche-Richtlinie (3. GW-RL)⁷⁶⁰ sowie
- die Geldtransferverordnung (GT-VO) oder Auftraggeberdaten-VO.⁷⁶¹

Die nationale Umsetzung der Richtlinie 2005/60/EG zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung („3. GW-RL“) erfolgte durch Novellierungen des Bankwesen-, des Börse-, des Versicherungsaufsichts- und des Wertpapieraufsichtsgesetzes 2007, was die Komplexität widerspiegelt, da sich diese Materie auf mehrere österr Gesetze verteilt. Die Geldwäschebestimmungen sollen vor allem auch die Bekämpfung organisierter und gewaltbegleiteter Schwerstkriminalität erleichtern. Dass bei Ermittlungen iZm Steuerstrafsachen oft andere Ziele verfolgt werden und deshalb besonderes Augenmaß hinsichtlich des grundrechtlichen Eingriffes erforderlich ist, wurde in Deutschland schon in den 90er Jahren erkannt.⁷⁶² Die Beachtung rechtsstaatlicher Mindestanfordernisse⁷⁶³ ist auch heute von großer Bedeutung.⁷⁶⁴

„Die Auftraggeberdaten-VO Nr 1781/2006 bestimmt, dass jede Überweisung mit einem vollständigen Kundendatensatz (Name, Adresse und Kontonummer) begleitet werden muss. Damit soll bewirkt werden, dass Geldtransfers lückenlos rückverfolgt werden können. (Ausnahmebestimmung können traditionelle Kleinbetragsspenden sein).“⁷⁶⁵

4. Elektronische Kommunikation

Die Datenschutzrichtlinie 1995/46/EG legt Datenschutzstandards für sämtliche EU-Rechtsakte fest, darunter auch für die Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation⁷⁶⁶, welche zuletzt durch die Richtlinie 2009/136/EG⁷⁶⁷ geändert wurde. Die

⁷⁶⁰ Richtlinie 2006/70/EG der Kommission vom 1. August 2006 mit Durchführungsbestimmungen für die Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates hinsichtlich der Begriffsbestimmung von politisch exponierten Personen und der Festlegung der technischen Kriterien für vereinfachte Sorgfaltspflichten sowie für die Befreiung in Fällen, in denen nur gelegentlich oder in sehr eingeschränktem Umfang Finanzgeschäfte getätigt werden (= ABI L 214 vom 4.8.2006, S 29–34).

⁷⁶¹ Verordnung (EG) Nr 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers (= ABI L 345 vom 8.12.2006, S 1-9).

⁷⁶² Herzog, Der Banker als Fahnder? Von der Verdachtsanzeige zur systematischen Verdachtsgewinnung – Entwicklungstendenzen der Geldwäschebekämpfung, WM 1996, 1753 (1754 f).

⁷⁶³ Herzog, Der Banker als Fahnder? Von der Verdachtsanzeige zur systematischen Verdachtsgewinnung – Entwicklungstendenzen der Geldwäschebekämpfung, WM 1996, 1753 (1763).

⁷⁶⁴ Vgl VI Grundrechtliche Analyse.

⁷⁶⁵ https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html#Rechtsgrundlagen_in_der_EU (Stand: 18.08.2013).

⁷⁶⁶ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (= ABI L 201 vom 31.7.2002, S 37-47).

⁷⁶⁷ Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen

RL zur elektronischen Kommunikation dient der Harmonisierung der Vorschriften der Mitgliedstaaten, damit ein gleichwertiger Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft gewährleistet werden kann.⁷⁶⁸ Sie stellt eine Detaillierung und Ergänzung der RL 1995/46/EG im Hinblick auf die genannten Zwecke dar und regelt auch den Schutz der berechtigten Interessen, bei denen es sich um juristische Personen handelt.⁷⁶⁹ Die RL 1995/46/EG gilt ua für nicht öffentliche Kommunikationsdienste.⁷⁷⁰

5. Weitere zu beachtende Vorschriften und Mitteilungen

- Der Rahmenbeschluss 2008/977/JI⁷⁷¹ vom Rat für Justiz und Inneres gilt für den grenzüberschreitenden Austausch von personenbezogenen Daten innerhalb der EU im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, nicht aber für die Datenverarbeitung innerhalb der Mitgliedstaaten. In der Praxis ist eine Trennung dieser Verarbeitungsvorgänge schwierig⁷⁷², was die Umsetzung und Anwendung des Rahmenbeschlusses erschweren kann.⁷⁷³
- Der Schutz der Privatsphäre und der Datenschutz sollen in den gesamten Technologie-Lebenszyklus integriert werden („Privacy by Design“). Dies beginnt im frühen

Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (= ABI L 337 vom 18.12.2009, S 11-36).

⁷⁶⁸ Vgl Art 1 Abs 1 der RL 2002/58/EG.

⁷⁶⁹ Art 1 Abs 2 der RL 2002/58/EG.

⁷⁷⁰ Vgl FN 6 in der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen (Gesamtkonzept für den Datenschutz in der Europäischen Union) vom 4.11.2010, KOM (2010) 609 endgültig.

⁷⁷¹ Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABI L 350 vom 30.12.2008, S 60-71). Der Rahmenbeschluss zielt nur auf eine Mindestharmonisierung der Datenschutzstandards.

⁷⁷² Eine solche Unterscheidung wird in den einschlägigen Instrumenten des Europarates nicht gemacht. Zu diesen Instrumenten gehören: Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr 108), Zusatzprotokoll zu diesem Übereinkommen betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV Nr 181) und Empfehlung R (87) 15 des Ministerkomitees des Europarates an die Mitgliedstaaten zur Regelung der Benutzung personenbezogener Daten durch die Polizei vom 17. September 1987.

⁷⁷³ Vgl Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen (Gesamtkonzept für den Datenschutz in der Europäischen Union) vom 4.11.2010, KOM (2010) 609 endgültig, S 15.

Entwurfsstadium und geht bis zu deren Einführung, Nutzung und letztendlichen Außerbetriebnahme.⁷⁷⁴

- Eine Änderung der Richtlinie 1995/46/EG wurde 2003 von der Europäischen Kommission abgelehnt. Zuvor eingebrachte Vorschläge Österreichs, Finnlands, Schwedens und des Vereinigten Königreichs beinhalteten zwar Bedenken, die Richtlinie könnte unter Umständen bestimmten technischen Entwicklungen nicht gerecht werden, sie enthielten aber keine konkreten Vorschläge, die in direktem Zusammenhang mit dieser Frage stehen.⁷⁷⁵ Die zurzeit in Diskussion befindliche Datenschutz-VO würde weitgehende Änderungen mit sich bringen.⁷⁷⁶
- Auf die vom Baseler Ausschuss der Bank für Internationalen Zahlungsausgleich (BIZ) beschlossenen datenschutzrechtlich relevanten Bereiche (vor allem im Reformpaket Basel II) werde ich in dieser Arbeit nicht eingehen und verweise auf bereits bestehende Literatur.⁷⁷⁷

6. SWIFT-Abkommen

a) Begriff

Das sog SWIFT-Abkommen ist ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus.⁷⁷⁸ Es will als „Mittel zum Schutz ihrer jeweiligen demokratischen Gesellschaften sowie ihrer gemeinsamen

⁷⁷⁴ Vgl Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen (Gesamtkonzept für den Datenschutz in der Europäischen Union) vom 4.11.2010, KOM (2010) 609 endgültig, S 13 mit Verweis auf Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre vom 2.5.2007, KOM (2007) 228 endgültig sowie Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine Digitale Agenda für Europa“ vom 26.8.2010, KOM (2010) 245 endgültig/2.

⁷⁷⁵ Erster Bericht der Kommission über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.5.2003, KOM (2003) 265 endgültig, S 22 et altera.

⁷⁷⁶ Vgl V.E Reform des „europäischen Datenschutzrechtes“.

⁷⁷⁷ Vgl insbesondere *Knyrim*, Datenschutzrechts-Compliance in der Bank – Die wichtigsten datenschutzrechtlichen Themen für Kreditinstitute, ÖBA 2007, 476 (479 bis 481), der darin einen guten Überblick zu Basel II und der damaligen bestehenden Literatur bietet. Basel III enthält vor allem neue Kapital- und Liquiditätsvorschriften, vgl zum Überblick die Informationen des deutschen Finanzministeriums: http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Service/Einfach_erklaert/2010-11-04-einfach-erklart-basel-III-flash-infografik.html (Stand: 18.08.2013).

⁷⁷⁸ Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= ABI L 195 vom 27.07.2010, S 5-14).

Werte, Rechte und Freiheiten den Terrorismus und seine Finanzierung insbesondere durch den Austausch von Informationen⁷⁷⁹ verhüten und bekämpfen.

In den einleitenden Bemerkungen des Abkommens⁷⁸⁰ wird darauf hingewiesen, dass das Programm des Finanzministeriums der Vereinigten Staaten von Amerika zum Aufspüren der Finanzierung des Terrorismus („TFTP“) „maßgeblich dazu beigetragen hat, Terroristen und deren Geldgeber zu ermitteln und festzunehmen, und zahlreiche sachdienliche Hinweise geliefert hat, die zu Zwecken der Terrorismusbekämpfung an die zuständigen Behörden in der ganzen Welt weitergegeben wurden und die für die Mitgliedstaaten der Europäischen Union von besonderem Nutzen waren“⁷⁸¹.

Nach dem Scheitern des Interimsabkommens, welches am 1.2.2010 hätte in Kraft treten und bis 31.10.2010 gültig sein sollen⁷⁸² wurde Kritik des deutschen Bundeskriminalamtes bekannt, welches die Weitergabe von Bankdaten an die Vereinigten Staaten von Amerika kritisierte. Mit Verweis auf einen Bericht im Nachrichtenmagazin „Der Spiegel“ hält die Ermittlungsbehörde den Datentransfer im Zuge des SWIFT-Abkommens bei der Bekämpfung des internationalen Terrorismus für nutzlos.⁷⁸³ Ein interner Vermerk des deutschen BKA beschreibt, dass „die aus fachlicher Sicht zu erwartenden Erkenntnisse aus einem systematischen und umfangreichen Abgleich der SWIFT-Daten zumindest für den Bereich der Finanzierung des Terrorismus <aus hiesiger Sicht nicht den mit der Datenrecherche verbundenen erheblichen materiellen und personellen Aufwand rechtfertigen>“⁷⁸⁴.

b) Historische Entwicklung

Seit Ende 2001 besteht ein Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP).⁷⁸⁵ 2006 wurde bekannt, dass die Vereinigten Staaten von Amerika auf die Daten des Unternehmens „SWIFT“ zurückgreifen, das bis dorthin Überweisungsdaten auch in den Vereinigten Staaten von Amerika gespeichert hatte.⁷⁸⁶ Daraufhin beschloss das Unternehmen „SWIFT“ wegen Datenschutzbedenken, „Überweisungen zwischen Europäern nur mehr in der Schweiz zu speichern, so dass das amerikanische Finanzministerium nur mehr Zugriff auf

⁷⁷⁹ ABl L 195 vom 27.07.2010, S 5.

⁷⁸⁰ Vgl ABl L 195 vom 27.07.2010, S 5-7.

⁷⁸¹ ABl L 195 vom 27.07.2010, S 5.

⁷⁸² Vgl weiter unten V.B.6.b) Historische Entwicklung.

⁷⁸³ *Tretter*, Der digital bewegte Mensch. Europäische Präsidentenkonferenz 2010, AnwBl 2010, 165 (168).

⁷⁸⁴ *Tretter*, Der digital bewegte Mensch. Europäische Präsidentenkonferenz 2010, AnwBl 2010, 165 (168 f) mit Verweis auf den online unter <http://www.spiegel.de/politik/deutschland/0,1518,669753,00.html> (Stand: 18.08.2013) zu findenden Artikel.

⁷⁸⁵ Vgl V.B.6.c) Inhalte des „SWIFT-Abkommens“.

⁷⁸⁶ *Urlesberger*, Europarecht: Das Neueste auf einen Blick, wbl 2010, 177 (180 f)., vgl bereits *Urlesberger*, Europarecht: Das Neueste auf einen Blick, wbl 2007, 224 (224).

Überweisungsdaten von und nach den Vereinigten Staaten hatte.“⁷⁸⁷ Die Vereinigten Staaten von Amerika drängten jedoch auch auf Mitteilung von Angaben über innereuropäische Überweisungen.⁷⁸⁸

Mit Schreiben des Finanzministeriums der Vereinigten Staaten von Amerika zum Thema SWIFT / Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP) vom 28.6.2007,⁷⁸⁹ welches an Peer Steinbrück⁷⁹⁰ und Franco Frattini⁷⁹¹ gerichtet war, verweist das Finanzministerium der Vereinigten Staaten von Amerika auf mehrere Zusicherungen⁷⁹², „in denen die Kontrollen und Garantien in Bezug auf den Umgang mit den Daten sowie auf ihre Verwendung und Verbreitung im Rahmen des Programms des Finanzministeriums zum Aufspüren der Finanzierung des Terrorismus (TFTP) dargelegt werden“⁷⁹³. Es wird betont, dass die dadurch ermittelten Daten lediglich zu Zwecken der Bekämpfung des Terrorismus verwendet werden und sie nur so lange gespeichert werden, als dies für die Zwecke der Terrorismusbekämpfung erforderlich ist, sowie dass alle Daten in gesicherter Umgebung aufbewahrt und ordnungsgemäß gehandhabt werden, was durch Stuart A. Levey⁷⁹⁴ zugesichert wird.

Das Antwortschreiben der Europäischen Union an das Finanzministerium der Vereinigten Staaten von Amerika⁷⁹⁵ bestätigt den Erhalt des Schreibens vom 28.6.2007 und begrüßt die einseitigen Zusicherungen der USA. Insbesondere verweist es auf die Einhaltung der Grundsätze des „sicheren Hafens“.⁷⁹⁶ Abschließend wird die Bemühung der Vereinigten Staaten von Amerika und der Europäischen Union, folgende Aspekte in Einklang zu bringen, gewürdigt: Wahrung der bürgerlichen Freiheiten, Bekämpfung des Terrorismus und ein reibungsloses Funktionieren des internationalen Finanzsystems.

⁷⁸⁷ *Urlesberger*, *Europarecht: Das Neueste auf einen Blick*, wbl 2010, 177 (181).

⁷⁸⁸ *Urlesberger*, *Europarecht: Das Neueste auf einen Blick*, wbl 2010, 177 (181).

⁷⁸⁹ Schreiben des Finanzministeriums der Vereinigten Staaten zum Thema SWIFT / Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP) (= ABI C 166 vom 20.07.2007, S 17-17)

⁷⁹⁰ Als damaliger Bundesminister der Finanzen der Bundesrepublik Deutschland war er Ratsvorsitzender der Finanzminister.

⁷⁹¹ Franco Frattini war zu dieser Zeit Vizepräsident der Europäischen Kommission.

⁷⁹² Vgl. Verarbeitung personenbezogener Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung - SWIFT (= ABI C 166 vom 20.07.2007, S 18-25).

⁷⁹³ ABI C 166 vom 20.07.2007, S 17.

⁷⁹⁴ Stuart A. Levey war von Juli 2004 bis März 2011 „Under Secretary for Terrorism and Financial Intelligence“. Dabei handelt es sich um eine Position im „United States Department of the Treasury“ (Finanzministerium der Vereinigten Staaten), welche für die Beendigung der finanziellen Unterstützung von Terroristen und die Beendigung der Finanzkriminalität, sowie für wirtschaftliche Sanktionen gegen „rogue nations“ (Schurkenstaaten) und die Bekämpfung der finanziellen Unterstützung für den Bau von Massenvernichtungswaffen zuständig ist. Die Ernennung erfolgt durch den Präsidenten der Vereinigten Staaten und muss durch den Senat bestätigt werden.

⁷⁹⁵ Antwortschreiben der Europäischen Union an das Finanzministerium der Vereinigten Staaten - SWIFT / Programm zum Aufspüren der Finanzierung des Terrorismus (ABI C 166 vom 20.07.2007, S 26-26).

⁷⁹⁶ Safe-Harbor-Regelung, vgl. weiter unten V.B.6.d) Exkurs: Safe Harbor.

In einem 2009 veröffentlichten deutschen Handbuch zum deutschen und europäischen Bankrecht wird erwähnt, dass zur datenschutzrechtlichen Lösung letztlich entweder das Rechenzentrum von SWIFT aus den USA in einen Staat der EU verlagert werden müsse oder ein völkerrechtlicher Vertrag mit den USA dem Datenschutz in Europa entsprechende Verfahren vorsehen müsse.⁷⁹⁷

In Österreich erlangte SWIFT jüngst durch das AktRÄG 2009⁷⁹⁸ Bedeutung: Gem § 13 Abs 3 und § 10a AktG genügt, wenn das AktG für eine Erklärung Schriftform vorschreibt, eine Erklärung in Textform, die über ein international verbreitetes, besonders gesichertes Kommunikationsnetz der Kreditinstitute, dessen Teilnehmer eindeutig identifiziert werden können, übermittelt wird.⁷⁹⁹ „Obwohl diese Erweiterung der Schriftform primär auf die Übermittlung von Depotbestätigungen abzielt, kommt sie auch für andere Erklärungen nach dem AktG in Betracht, beispielsweise für die Berufung der Depotbank auf die ihr erteilte Vollmacht gemäß § 114 Abs 1 vierter Satz AktG.“⁸⁰⁰

Im März 2008 gab die Kommission die Ernennung des Richters Jean-Louis Bruguière als „renommierte europäische Persönlichkeit“ bekannt, dessen Aufgabe es war, zu prüfen, ob das TFTP im Einklang mit den Zusicherungen umgesetzt wird. Den ersten Bericht legte Bruguière im Dezember 2008 vor, der im Februar 2009 dem Rat der Justiz- und Innenminister und im September 2009 dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments vorgelegt wurde.

Die Europäische Kommission fasste daraufhin einen Beschlussvorschlag,⁸⁰¹ woraufhin der Rat am 30.11.2009 die Unterzeichnung des Abkommens zur Weitergabe von

⁷⁹⁷ Rudolf/Kötterheinrich in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, § 5, Rz 21, S 150.

⁷⁹⁸ BGBl. I Nr. 71/2009: Bundesgesetz, mit dem das Aktiengesetz 1965, das SE-Gesetz, das Unternehmensgesetzbuch, das Umwandlungsgesetz, das Spaltungsgesetz, das Kapitalberichtigungsgesetz, das Gesellschafter-Ausschlussgesetz, das Übernahmegesetz, das Genossenschaftsrevisionsgesetz und das Grundbuchgesetz geändert werden (Aktienrechts-Änderungsgesetz 2009 – AktRÄG 2009).

⁷⁹⁹ Vgl auch *Bachner*, Aktienrechts-Änderungsgesetz beschlossen! – Die wichtigsten Neuerungen, GeS 2009, 248 (250).

⁸⁰⁰ Zu weiteren Einzelheiten („SWIFT opt-out“ und „Fax opt-in“) in diesem Zusammenhang: *Bachner*, Aktienrechts-Änderungsgesetz beschlossen! – Die wichtigsten Neuerungen, GeS 2009, 248 (250) sowie *Potyka*, Die Hauptversammlung nach dem AktRÄG 2009. Einführung verschiedener Formen der elektronischen Teilnahme und des Nachweisstichtagssystems, CFOaktuell 2009, 174 (176 f).

⁸⁰¹ KomVorschlag vom 17.12.2009 für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= KOM/2009/703 endg, dem Europäischen Parlament unterbreitet unter 5303/1/2010 REV).

Überweisungsdaten beschloss.⁸⁰² Das Europäische Parlament nahm zum SWIFT-Abkommen bereits am 17.9.2009 Stellung.⁸⁰³

Dieses Abkommen hätte am 1.2.2010 als Interimsabkommen für neun Monate lang in Kraft treten sollen, wobei das Europäische Parlament die Zustimmung am 11.2.2010 verweigerte.⁸⁰⁴

Die beiden zuständigen Kommissarinnen Malmström (Inneres) und Reding (Justiz) hielten an einem solchen Abkommen fest⁸⁰⁵ und überwanden durch die starke Einbindung des Europäischen Parlaments die Widerstände gegen das Abkommen.⁸⁰⁶ Die Europäische Kommission nahm am 24.03.2010 eine Empfehlung an den Rat an zur Genehmigung der Aufnahme von Verhandlungen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika zur Bereitstellung von Zahlungsverkehrsdaten an das Finanzministerium der Vereinigten Staaten von Amerika zu Zwecken der Verhütung und Bekämpfung des Terrorismus und der Terrorismusfinanzierung, worauf der Rat am 11.5.2010 einen Beschluss mit Verhandlungsrichtlinien, in dem die Kommission zur Aufnahme von Verhandlungen im Namen der Europäischen Union ermächtigt wurde, erließ.⁸⁰⁷ Das Europäischen Parlament verabschiedete am 5.5.2010 eine Entschließung⁸⁰⁸ zu der Empfehlung der Kommission an den Rat zur Genehmigung der Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika zur Übermittlung von Zahlungsverkehrsdaten an das US-Finanzministerium zu Zwecken der Verhütung und

⁸⁰² Vgl. *Urlesberger*, Europarecht: Das Neueste auf einen Blick, wbl 2010, 177 (181) mit Verweis auf die genannten Beschlüsse mit Verweis auf Beschluss 2010/16/GASP/JI des Rates vom 30. November 2009 über die Unterzeichnung - im Namen der Europäischen Union - des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= ABI L 8 vom 13.01.2010, S 9-10), damaliger Entwurf des Abkommens vgl. ABI L 8 vom 13.01.2010, S 9-16.

⁸⁰³ SWIFT Entschließung des Europäischen Parlaments vom 17. September 2009 zu dem geplanten internationalen Abkommen, demgemäß dem Finanzministerium der Vereinigten Staaten Finanztransaktionsdaten zum Zwecke der Prävention und Bekämpfung des Terrorismus und der Terrorismusfinanzierung zur Verfügung gestellt werden sollen (= ABI C 224E vom 19.08.2010, S 8-11).

⁸⁰⁴ Vgl. Legislative Entschließung des Europäischen Parlaments vom 11. Februar 2010 zu dem Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= ABI C 341E vom 16.12.2010, S 100).

⁸⁰⁵ IP/10/152 vom 11.2.2010 (= Pressemitteilung).

⁸⁰⁶ Vgl. zur Chronologie: *Urlesberger*, Europarecht: Das Neueste auf einen Blick, wbl 2010, 177 (181).

⁸⁰⁷ Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= KOM/2010/317 endg).

⁸⁰⁸ SWIFT Entschließung des Europäischen Parlaments vom 5. Mai 2010 zu den Empfehlungen der Kommission an den Rat betreffend die Ermächtigung zur Aufnahme von Verhandlungen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über ein internationales Abkommen über die Bereitstellung von Daten über Finanztransaktionen für das Finanzministerium der Vereinigten Staaten zu Zwecken der Verhütung und Bekämpfung des Terrorismus und der Terrorismusfinanzierung (= ABI C 81E vom 15.03.2011, S 66-70).

Bekämpfung des Terrorismus und der Terrorismusfinanzierung. Am 11.6.2010 wurde das Abkommen paraphiert. Die Laufzeit beträgt fünf Jahre. Das Abkommen mit den Vereinigten Staaten von Amerika über die Übermittlung und Verarbeitung von Zahlungsverkehrsdaten trat am 1.8.2010 in Kraft.⁸⁰⁹ Bereits damals nahmen mehr als 9000 Banken und andere Unternehmen an SWIFT teil.⁸¹⁰

Anzumerken ist aber, dass in den USA eine der EU-Datenschutz-RL entsprechende umfassende Datenschutzgesetzgebung („omnibus privacy law“) für den nichtstaatlichen Sektor fehlt und der geltende Privacy Act von 1974 sowie der Freedom of Information Act (FOIA) nur für Bundesbehörden gilt.⁸¹¹

c) Inhalte des „SWIFT-Abkommens“

TFTP - Terrorist Finance Tracking Program

Das Programm des US-Finanzministeriums zum Aufspüren der Finanzierung des Terrorismus („TFTP“) wurde kurz nach den Terroranschlägen des 11. September 2001 vom US-Finanzministerium eingerichtet.⁸¹² Im Rahmen des TFTP erließ das US-Finanzministerium administrative Anordnungen gegen SWIFT auf Herausgabe bestimmter Aufzeichnungen über Finanztransaktionen. Öffentliche Medien legten TFTP im Juni 2006 offen, wobei scharfe Kritik an TFTP und dem dadurch erfolgten Austausch von Daten geäußert wurde.⁸¹³

TFTP hat nach Ansicht der Europäischen Union maßgeblich dazu beigetragen, Terroristen und deren Geldgeber zu ermitteln und festzunehmen, und zudem zahlreiche sachdienliche Hinweise geliefert, die zu Zwecken der Terrorismusbekämpfung an die zuständigen Behörden in der ganzen Welt weitergegeben wurden und für die Mitgliedstaaten der Europäischen Union von besonderem Nutzen waren.⁸¹⁴

Aus grundrechtlicher Sicht sind die durch TFTP erfolgten Einschränkungen mE sehr kritisch zu beurteilen. Es wurde jahrelang auf europäische Überweisungsdaten zugegriffen, die

⁸⁰⁹ Vgl auch *Urbantschitsch/Hofer*, Terrorismusbekämpfung, *ecolex* 2010, 917 (917).

⁸¹⁰ *Kurioses & Wissenswertes*, SWIFT-Abkommen zum Transfer von Finanzdaten in Kraft getreten, *jusIT* 2010, 162 mit Verweis auf <http://www.heise.de/newsticker/meldung/SWIFT-Abkommen-zum-Finanzdatentransfer-tritt-in-Kraft-1048817.html> (Stand: 18.08.2013) und <http://register.consilium.europa.eu/pdf/en/10/st11/st11222-re01.en10.pdf> - Council Decision der EU (Stand: 18.08.2013).

⁸¹¹ *Kastelitz*, Transatlantischer Datenschutzrechts-Dialog - ein Erfahrungsbericht, *jusIT* 2010, 180 (181).

⁸¹² Vgl Verarbeitung personenbezogener Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung - SWIFT (= *ABl C* 166 vom 20.7.2007, S 18).

⁸¹³ Verarbeitung personenbezogener Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung - SWIFT (= *ABl C* 166 vom 20.7.2007, S 19).

⁸¹⁴ Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= *ABl L* 195 vom 27.7.2010, S 5).

SWIFT auf Servern in den USA gespeichert hatte. Erst der aufgrund der öffentlichen Berichterstattung erhöhte Druck durch die Öffentlichkeit schränkte den Zugriff auf europäische Überweisungsdaten ein. Die Rechtskonformität mit der Datenschutzrichtlinie bestand somit nicht. Der Schutz personenbezogener Daten musste dem Interesse an Terrorismusbekämpfung weichen, ohne jedoch eine Verhältnismäßigkeitsprüfung vorzunehmen.

Ähnliche Bestrebungen erfolgten auch in Deutschland, wo am 1. Juli 2002 das Gesetz zur Fortentwicklung des Finanzplatzes Deutschland⁸¹⁵ in Kraft trat. Unter diesem revolutionär anmutenden Titel wurde auch § 24c (Automatisierter Abruf von Kontoinformationen) in das deutsche Kreditwesengesetz⁸¹⁶ eingefügt, der vorsieht, dass die deutschen Kreditinstitute ab 1. April 2003 verpflichtet sind, die Stammdaten aller gemäß § 154 AO⁸¹⁷ legitimationsgeprüften Konten und/oder Depots auf einer Plattform zu hinterlegen.⁸¹⁸ Im Ergebnis ermöglicht diese Regelung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und den Finanzbehörden, den Namen eines Steuerpflichtigen innerhalb kürzester Zeit mit allen bei allen Kreditinstituten vorhandenen Kontenstammdaten abzugleichen und somit Abweichungen mit den der Steuererklärung beigefügten Jahressteuerbescheinigungen der Kreditinstitute festzustellen.⁸¹⁹ Unter der anfänglichen Bestrebung der Bekämpfung des international operierenden Terrorismus wurde durch den deutschen Gesetzgeber eine Abfragemöglichkeit für sämtliche Strafverfolgungsorgane durch Zugriff auf die Daten aller legitimationsgeprüften Konten begründet.⁸²⁰ Durch die Formulierung „soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist“ wurde die Bestimmung des § 24c Abs 3 Z 2⁸²¹ deutsches KWG vom deutschen Bundesverfassungsgericht als mit dem

⁸¹⁵ Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Deutsches BGBI 2002 I, Nr 39, S 2010), vgl besonders S 2046 und S 2053 f (Viertes Finanzmarktförderungsgesetz).

⁸¹⁶ Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (Deutsches BGBI 1998 I, Nr 62, S 2776), das zuletzt durch Artikel 2 des Gesetzes vom 24. Februar 2012 (Deutsches BGBI 2012 I, Nr 10, S 206) geändert worden ist (KWG).

⁸¹⁷ Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (Deutsches BGBI 2002 I, Nr 72, S 3866; 2003 I, Nr 2, S 61), die zuletzt durch Artikel 2 Absatz 71 des Gesetzes vom 7. August 2013 (Deutsches BGBI 2013 I, Nr 48, S 3154) geändert worden ist (AO).

⁸¹⁸ Vgl *Zubrod*, Automatisierter Abruf von Kontoinformationen nach § 24c KWG - Rechtliche Voraussetzungen und Grenzen, WM 2003, 1210 (1210).

⁸¹⁹ *Zubrod*, Automatisierter Abruf von Kontoinformationen nach § 24c KWG - Rechtliche Voraussetzungen und Grenzen, WM 2003, 1210 (1213).

⁸²⁰ *Zubrod*, Automatisierter Abruf von Kontoinformationen nach § 24c KWG - Rechtliche Voraussetzungen und Grenzen, WM 2003, 1210 (1214).

⁸²¹ Die Bundesanstalt erteilt auf Ersuchen Auskunft aus der Datei nach Absatz 1 Satz 1 (...) 2. den für die Leistung der internationalen Rechtshilfe in Strafsachen sowie im Übrigen für die Verfolgung und Ahndung von Straftaten zuständigen Behörden oder Gerichten, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist (...).

deutschen Grundgesetz vereinbar angesehen.⁸²² Generalklauselartige Einschränkungen ermöglichen hierbei einen sehr weiten Ermessensspielraum.

§ 24c Abs 3 Satz 1 Z 2 deutsches KWG erlaubt Kontenabrufe nur im Rahmen von konkreten Ermittlungs- oder Rechtshilfeverfahren, die einen Anfangsverdacht einer Straftat oder ein Rechtshilfeersuchen voraussetzen. Routinemäßige Abrufe nach § 93 Abs 7 deutsche AO „ins Blaue hinein“ sind somit unzulässig.⁸²³

Voraussetzungen für das Ersuchen der Vereinigten Staaten von Amerika:

Im nun geltenden sog SWIFT-Abkommen⁸²⁴ sind die Voraussetzungen für ein Ersuchen der Vereinigten Staaten von Amerika geregelt. Das US-Finanzministerium stellt nach Maßgabe des Rechts der Vereinigten Staaten von Amerika einem bezeichneten Anbieter im Hoheitsgebiet der Vereinigten Staaten von Amerika nachstehend als „Ersuchen“ bezeichnete Vorlageordnungen (production orders) zu, um im Gebiet der Europäischen Union gespeicherte Daten zu erlangen, die zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Terrorismus und Terrorismusfinanzierung notwendig sind.⁸²⁵ Das Ersuchen muss folgende Kriterien erfüllen:⁸²⁶

- a) *Die angeforderten Daten, die zur Verhütung, Ermittlung, Aufdeckung und Verfolgung von Terrorismus und Terrorismusfinanzierung notwendig sind, müssen möglichst präzise unter Angabe der Datenkategorien bezeichnet werden.*
- b) *Es muss klar begründet werden, warum die Daten notwendig sind.*
- c) *Das Ersuchen muss so eng wie möglich gefasst sein, um die Menge der angeforderten Daten auf ein Minimum zu beschränken, wobei den Analysen früherer und gegenwärtiger Terrorrisiken anhand der Art der Daten und geografischer Kriterien sowie den Erkenntnissen über terroristische Bedrohungen und Schwachstellen, geografischen Analysen sowie Bedrohungs- und Gefährdungsanalysen gebührend Rechnung zu tragen ist.*
- d) *Es dürfen keine Daten angefordert werden, die sich auf den Einheitlichen Euro-Zahlungsverkehrsraum beziehen.*

⁸²² BVerfGE vom 13.6.2007 - 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05.

⁸²³ BVerfGE vom 13.6.2007 - 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05; Rz 144.

⁸²⁴ Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (= ABI L 195 vom 27.7.2010, S 5-14).

⁸²⁵ Vgl Art 4 Abs 1 des SWIFT-Abkommens 2010.

⁸²⁶ Vgl Art 4 Abs 2 lit a bis d des SWIFT-Abkommens 2010.

Eine Schlüsselfunktion kommt Europol zu. Nach Art 4 Abs 4 bis 5 leg cit prüft Europol, ob die Voraussetzungen des Art 4 Abs 2 des SWIFT-Abkommens vorliegen und erteilt bei Erfüllung der Voraussetzungen die Bestätigung. Die Bestätigung verpflichtet den Anbieter (SWIFT) dazu, dem US-Finanzministerium die Daten bereitzustellen. Art 5 des Abkommens definiert die Garantien für die Verarbeitung bereitgestellter Daten.

ME wird hier unter dem Titel der „Terrorismusbekämpfung“ eine weitgehende Einschränkung von Grundrechten vollzogen, deren Verstöße nur schwer kontrollierbar sind. Dies verwundert mich umso mehr, als das Recht auf Auskunft in Art 15 Abs 1 des Abkommens als Recht auf eine Bestätigung verstanden wird, dass alle erforderlichen Überprüfungen durchgeführt wurden, um sicherzustellen, dass die Datenschutzrechte nach dem Abkommen beachtet wurden und dass insbesondere keine gegen dieses Abkommen verstoßende Verarbeitung von personenbezogenen Daten stattgefunden hat.⁸²⁷

Art 15 Abs 2 des Abkommens normiert, dass die Offenlegung der auf der Grundlage dieses Abkommens verarbeiteten personenbezogenen Daten gegenüber der betroffenen Person angemessenen rechtlichen Beschränkungen unterworfen werden kann, die nach Maßgabe des einzelstaatlichen Rechts im Interesse der Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten und zum Schutz der öffentlichen oder nationalen Sicherheit unter gebührender Beachtung des berechtigten Interesses der betroffenen Person anwendbar sind. Positiv zu bewerten ist, dass im Fall der Verweigerung oder Einschränkung der Offenlegung der personenbezogenen Daten dies vom Datenschutzbeauftragten des US-Finanzministeriums schriftlich zu erläutern und mit einer Belehrung über die in den Vereinigten Staaten von Amerika verfügbaren administrativen und gerichtlichen Rechtsbehelfe zu versehen ist.

Dass die Europol zustehende Genehmigungsbefugnis nicht eingehend schriftlich dokumentiert ist, ergibt sich aus der am 4.3.2011 veröffentlichten Mitteilung des Europol Joint Supervisory Body⁸²⁸ (JSB).⁸²⁹ Der Überprüfungsbericht ist in englischer Sprache abrufbar.⁸³⁰ Dort wird kritisiert, dass die Anfragen an Europol beinahe identisch in Bezug auf ihre Art sind und umfassende Datensätze, die auch Daten von EU-Mitgliedstaaten beinhalten, umfassen. Eine neuerliche Überprüfung im November 2011 hat einen weiteren Abschlussbericht ergeben, der versucht, allgemeine nicht der Geheimhaltungspflicht

⁸²⁷ Vgl Art 15 Abs 1 des SWIFT-Abkommens.

⁸²⁸ Auf Deutsch: Gemeinsame Kontrollinstanz von Europol (GKI).

⁸²⁹ <http://europoljsb.consilium.europa.eu/about.aspx> (Stand: 18.08.2013).

⁸³⁰ <http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=de> (Stand: 18.08.2013).

unterliegende Schlussfolgerungen der Überprüfung darzulegen.⁸³¹ Darin wird abermals betont, dass die Vereinigten Staaten von Amerika den Informationsgehalt ihrer Ersuchen erhöhen müssen und so etwa genauer begründen müssen, warum der gewählte geografische Bereich, die angeforderten einzelnen Datenkategorien und die tatsächlichen Daten in der jeweils angeforderten Art der Meldung benötigt werden.⁸³² Notwendig ist demnach „mehr Transparenz gegenüber Dritten, darunter auch die breite Öffentlichkeit“⁸³³.

Diese deutliche Wortwahl der Gemeinsamen Kontrollinstanz von Europol lässt mE klare Schlussfolgerungen zu:

- 1) Um erteilte Genehmigung im Nachhinein überprüfen zu können, müssen nachvollziehbare schriftliche Aufzeichnungen über die Ersuchen geführt werden, die eine nachträgliche Beurteilung der Entscheidungsfindung ermöglichen.
- 2) Der hohe Geheimhaltungsgrad erschwert die Offenlegung gegenüber Dritten und somit auch gegenüber der Öffentlichkeit. Dies muss durch weitgehende Kontrollbefugnisse des Datenschutzbeauftragten und der Gemeinsamen Kontrollinstanz von Europol ausgeglichen werden.
- 3) Die bestehenden Auskunftsrechte nach dem SWIFT-Abkommen ermöglichen durch die Einschränkung der „angemessenen rechtlichen Beschränkungen“ de facto kein Auskunftsrecht der Betroffenen, was eine effektive Strafverfolgung ermöglichen soll. Dies müsste durch weiterreichende nachträgliche Auskunftspflichten gegenüber den Betroffenen ausgeglichen werden.

Änderung der Rechtsetzungskompetenz:

Durch den Vertrag von Lissabon wurde in Art 218 Abs 6 lit a AEUV normiert, dass das Europäische Parlament in mehreren Fällen zuzustimmen hat, bevor der Rat den Beschluss über den Abschluss einer Übereinkunft fassen kann. Darunter findet sich ua die Zustimmung zu Übereinkünften, die durch die Einführung von Zusammenarbeitsverfahren einen besonderen institutionellen Rahmen schaffen.

⁸³¹ <http://europoljsb.consilium.europa.eu/media/207866/tftp%20public%20statement%20-%20final%20-%20march%202012.de.pdf> (Stand: 18.08.2013).

⁸³² Vgl. <http://europoljsb.consilium.europa.eu/media/207866/tftp%20public%20statement%20-%20final%20-%20march%202012.de.pdf>, Seite 3 (Stand: 18.08.2013).

⁸³³ Vgl. <http://europoljsb.consilium.europa.eu/media/207866/tftp%20public%20statement%20-%20final%20-%20march%202012.de.pdf>, Seite 4 (Stand: 18.08.2013)

Am 11. Februar 2010 hat das Plenum des Europäischen Parlaments in Straßburg erstmals in der Geschichte des Parlaments einen Vertragstext der Kommission und des Rates zurückgewiesen.⁸³⁴

Am 8. Juli 2010 stimmte das Europäische Parlament dann einer abgeänderten Fassung des SWIFT-Abkommens mehrheitlich zu.⁸³⁵ Es verweist darin insbesondere auf die in Art 12 Abs 1 des Abkommens vorgesehene unabhängige Person der Europäischen Union und die Empfehlung an die Europäische Kommission, möglichst bald eine Auswahl von drei Bewerbern für diese Position dem EP und dem Rat vorzulegen.⁸³⁶ Unabhängige Prüfer, einschließlich einer von der Europäischen Kommission ernannten Person, haben zu überprüfen, ob die strenge Zweckbeschränkung auf die Terrorismusbekämpfung sowie die anderen Garantien in den Artikeln 5 und 6 des Abkommens eingehalten werden.⁸³⁷ Damit sind relativ weitgehende Befugnisse verbunden.⁸³⁸

Bezeichnete(r) Anbieter laut Anhang:

Art 3 des Abkommens normiert die Verpflichtung der (Vertrags-) Parteien, dafür zu sorgen, dass die von den Parteien auf der Grundlage dieses Abkommens gemeinsam als Anbieter von internationalen Zahlungsverkehrsdiensten bezeichneten Stellen („bezeichnete Anbieter“) dem US-Finanzministerium angeforderte Zahlungsverkehrsdaten und damit verbundene Daten, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Terrorismus und Terrorismusfinanzierung notwendig sind, bereitstellen („bereitgestellte Daten“). Es entsteht der Eindruck, als ob es mehrere internationale Anbieter von Zahlungsverkehrsdiensten gibt. Die Liste der bezeichneten Anbieter, die dem Abkommen beigelegt ist, enthält jedoch nur einen bezeichneten Anbieter: Society for Worldwide Interbank Financial Telecommunication (SWIFT). Aus diesem Grund ist das Abkommen auch als SWIFT-Abkommen bekannt.

d) Exkurs: Safe Harbor

Dieses von *David Aaron* mitentwickelte Konzept beruht darauf, Datenschutzerfordernungen zu definieren, dessen Akzeptanz und effektive Einhaltung die Vermutung eines angemessenen

⁸³⁴ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0029+0+DOC+XML+V0//DE&language=DE> (Stand: 18.08.2013).

⁸³⁵ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0279+0+DOC+XML+V0//DE&language=DE> (Stand: 18.08.2013).

⁸³⁶ Vgl 2. Punkt der legislativen Entschließung vom 8. Juli 2010.

⁸³⁷ Vgl Art 12 Abs 1 Satz 1 des SWIFT-Abkommens.

⁸³⁸ Vgl Art 12 Abs 1 Satz 2 und 3 des SWIFT-Abkommens.

Schutzniveaus verschafft.⁸³⁹ Dadurch konnte eine Lösung geschaffen werden, die die strukturellen Unterschiede der Vereinigten Staaten von Amerika und der Europäischen Union überwindet und so die Übermittlung von Daten aus der EU in die USA ermöglicht.

„Safe Harbor besteht im Wesentlichen aus sieben Prinzipien, zu deren Einhaltung sich US-Unternehmen freiwillig verpflichten können, soweit sie personenbezogene Daten aus dem Gebiet der EU erhalten und verarbeiten.“⁸⁴⁰ Die Unternehmen verpflichten sich aber auch dazu, die verbindlichen Frequently Asked Questions (FAQ) zu beachten.⁸⁴¹ Welche Unternehmen sich den Safe-Harbor-Grundsätzen verpflichtet haben, kann auf einer Webseite abgerufen werden.⁸⁴²

Alternativen zur Erklärung der Einhaltung der Safe-Harbor-Grundsätze stellen die Standardvertragsklauseln⁸⁴³ sowie die Binding Corporate Rules (BCR) dar, wobei beide von der DSK genehmigt werden müssen.⁸⁴⁴

Die komplexe Regelung des internationalen Datenaustausches führt in der Praxis immer wieder zu Unklarheiten und Unsicherheiten bei österreichischen Rechtsanwendern.⁸⁴⁵ So werden etwa Anträge auf Genehmigung eines Datentransfers zu einem „Safe Harbor“ – Unternehmen bei der österr DSK eingebracht, welche – da ja keine Genehmigungspflicht besteht – von der DSK abgewiesen werden.⁸⁴⁶

⁸³⁹ Brühann in Büllesbach (Hrsg), Datenverkehr ohne Datenschutz?, 47.

⁸⁴⁰ Westphal in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 74.

⁸⁴¹ Jahnle, Handbuch Datenschutzrecht, 4/140.

⁸⁴² Vgl <http://www.export.gov/safeharbor> (Stand: 18.08.2013).

⁸⁴³ Vgl V.A.5.c) Übermittlung und Überlassung.

⁸⁴⁴ Zur Übermittlung von Mitarbeiterdaten im Konzern: Oberhofer in Bauer/Reimer (Hg), Handbuch Datenschutzrecht (2009) 499 f; bei Übermittlung von Mitarbeiterdaten von Österreich an eine amerikanische Konzernmutter, besteht auch bei Unterwerfung der Konzernmutter unter die Safe-Harbor-Grundsätze eine Meldepflicht gemäß §§ 17 ff DSG, aaO.

⁸⁴⁵ Dies konstatiert Leissler in Leissler, Und die Daten fließen über den Atlantik..., eolex 2007, 747 (749).

⁸⁴⁶ Leissler in Leissler, Und die Daten fließen über den Atlantik..., eolex 2007, 747 (750).

C. EDI und SEPA

1. EDI – Elektronischer Datenaustausch

„Unter EDI (Abkürzung für engl: *electronic data interchange*) versteht man den elektronischen Datenaustausch über Geschäftstransaktionen (Bestellungen, Rechnungen, Überweisungen, Warenerklärungen usw) zwischen Betrieben. Die Daten werden in Form von strukturierten, nach vereinbarten Regeln formatierten Nachrichten übertragen. Dadurch ist es dem Empfänger möglich, die Daten direkt in seinen Anwendungsprogrammen weiterzuverarbeiten (Durchgängigkeit der Daten).“⁸⁴⁷

Bei EDI müssen Daten nur ein einziges Mal erfasst werden und können dann automatisiert weiter verarbeitet werden. Dadurch können sog „Medienbrüche“ vermieden werden, wodurch eine erhebliche Zeitersparnis und eine Reduzierung der Fehlerquellen entsteht.⁸⁴⁸

EDI bezeichnet nicht ein spezielles Verfahren oder eine bestimmte Technik, sondern steht für eine Vielzahl von Standards und Abläufen zum Austausch elektronischer Dokumente.⁸⁴⁹

Heute wird oft das Internet als Netzwerk-Infrastruktur für die Übertragung von EDI-Nachrichten genutzt.⁸⁵⁰

EDI benötigt einheitliche Normen für den Inhalt und die Syntax von elektronisch zu übertragenden Daten. Deshalb arbeiten seit Anfang der 1980er Jahre internationale Gremien⁸⁵¹ an einer Vereinheitlichung der EDI-Verfahren. Die EDIFACT-Normen⁸⁵² sind Ergebnis dieser Bestrebungen.⁸⁵³

In jüngster Zeit wurde eine Reihe neuer EDI-Standards entwickelt, die einfacher aufgebaut und nicht nur maschinell verarbeitbar sind, sondern auch einfach mittels Webbrowser

⁸⁴⁷ Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 958.

⁸⁴⁸ Vgl Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 958.

⁸⁴⁹ Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 958.

⁸⁵⁰ Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 960; zu den vertragsrechtlichen Rahmenbedingungen für einen funktionierenden rechtsgeschäftlichen Verkehr vgl bereits Brenn, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ 1997, 641 (651 ff).

⁸⁵¹ Besonders zu erwähnen ist hierbei die Organisation der Vereinten Nationen (UNO).

⁸⁵² EDIFACT (Abkürzung von engl: *electronic data interchange for administration, commerce and transport*; elektronischer Datenaustausch für Verwaltung, Handel und Transport) bezeichnet eine aufeinander abgestimmte Grundgesamtheit internationaler Normen für die Darstellung von Geschäfts- und Handelsdaten beim elektronischen Datenaustausch zwischen Betrieben – vgl Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 961.

⁸⁵³ Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 961.

darstellbar sind. Hierbei sind zwei praxisrelevante Ansätze zu nennen: Web-EDI⁸⁵⁴ und XML/EDI^{855, 856}.

Beim elektronischen Datenaustausch im Zusammenhang mit EDI-Standards wird zwischen folgenden Standards unterschieden:⁸⁵⁷

- Identifikationsstandards zur Identifikation von Produkten und Unternehmen,
- Klassifikationsstandards zur einfachen Suche nach Produkten,
- Katalogstandards zum Datenaustausch zwischen Anbietern und Kunden,
- Transaktionsstandards als Basis zur Automatisierung von Geschäftsprozessen und
- Prozesstandards zur Ermöglichung der Automatisierung komplexer Geschäftsabläufe.

EDI ist im Zusammenhang mit SCM⁸⁵⁸ zu sehen. Um die Lieferkette vom ersten Rohstofflieferanten bis zum Endverbraucher möglichst effizient und kostengünstig zu gestalten, ist eine intensive Zusammenarbeit zwischen den beteiligten Betrieben zur gemeinsamen, bestmöglichen Gestaltung aller inner- und überbetrieblichen Material-, Informations- und Geldflüsse notwendig.⁸⁵⁹

Diese Effizienzsteigerung ist auch der Grund für den Einsatz des automatischen Informationsaustausches im Bereich der Finanzdienstleistungen, um mögliche Steuerhinterziehungen durch zB die Nicht-Versteuerung von Zinserträgen in anderen EU-Mitgliedsstaaten rasch aufdecken zu können.

⁸⁵⁴ Hierbei „werden Geschäftsdaten in ein HTML-Formular im Browser eingegeben, welche danach in eine standardisierte EDI-Nachricht konvertiert werden. Diese Daten werden an den Geschäftspartner übermittelt, der die Informationen wie eine herkömmliche EDI-Nachricht automatisiert weiterverarbeiten kann.“ (Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 961)

⁸⁵⁵ „XML/EDI bezeichnet die Nutzung der XML-Technik für den elektronischen Austausch strukturierter Geschäftsnachrichten. Es stellt ein Framework für unterschiedliche Datentypen, zum Beispiel Rechnungen, Lieferanten usw dar, das es erlaubt, Daten konsistent zu suchen, decodieren, manipulieren und darzustellen. EDI-Nachrichten können auch erweitert und um zusätzliche Elemente ergänzt werden.“ (Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 962).

⁸⁵⁶ Vgl für weitere Details: Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 961 ff.

⁸⁵⁷ Vgl im Folgenden sowie zur Belegung mit Zahlen zur praktischen Verbreitung und zumeist verwendete Standards: Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 992 ff.

⁸⁵⁸ Supply-Chain-Management bzw Lieferkettenmanagement.

⁸⁵⁹ Hansen/Neumann, Wirtschaftsinformatik 1¹⁰, 947.

2. SEPA – Single European Payment Area

SEPA ist im Zusammenhang mit der sog Zahlungsdiensterichtlinie⁸⁶⁰, welche im österr ZaDiG⁸⁶¹ umgesetzt wurde, zu sehen. Das Ziel besteht darin, einen einheitlichen europäischen Zahlungsraum (Single European Payment Area – SEPA) zu schaffen. Dadurch sollen vor allem innereuropäische Überweisungen schneller und kostengünstiger abgewickelt werden.⁸⁶²

Um die unterschiedlichen nationalen Rechtsvorschriften, insbesondere in Bezug auf Ausführungsfristen und Haftungen, einander anzugleichen, wurde 2007 vom Europäischen Parlament und vom Rat die Zahlungsdiensterichtlinie beschlossen. Auf der Grundlage der durch PSD erfolgten Harmonisierung der Bedingungen für die Erbringung von Zahlungsdienstleistungen kann die europäische Bankwirtschaft in Zusammenarbeit mit der Europäischen Zentralbank und der Europäischen Kommission weiter an der Realisierung des einheitlichen europäischen Zahlungsraums arbeiten.⁸⁶³

Durch die Einführung des SEPA-Lastschriftverfahrens sollen in den europäischen Teilnehmerländern des einheitlichen Euro-Zahlungsverkehrsraumes (kurz SEPA) Rechnungen per Lastschrift beglichen werden können.⁸⁶⁴

Heute nehmen folgende Staaten am Projekt des einheitlichen Euro-Zahlungsverkehrsraumes teil: Die 27 Mitgliedstaaten der Europäischen Union, die drei weiteren Staaten des Europäischen Wirtschaftsraumes (Island, Liechtenstein, Norwegen), sowie Schweiz und Monaco.

SEPA soll den Zahlungsverkehr in der EU völlig neu gestalten, wodurch der Zahlungsverkehr für die Kunden wesentlich transparenter, einfacher und schneller werden soll.⁸⁶⁵

⁸⁶⁰ Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (= ABl L 319 vom 5.12.2007, S 1–36), Payment Services Directive (PSD).

⁸⁶¹ BGBl I Nr 66/2009, zuletzt geändert durch BGBl I Nr 70/2013: Bundesgesetz, mit dem ein Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG) erlassen und das Bankwesengesetz, das Fern-Finanzdienstleistungs-Gesetz, das Konsumentenschutzgesetz, das Finanzmarktaufsichtsbehördengesetz, das Versicherungsaufsichtsgesetz und das Wertpapieraufsichtsgesetz 2007 geändert werden sowie das Überweisungsgesetz aufgehoben wird.

⁸⁶² <http://www.fma.gv.at/de/unternehmen/zahlungsinstitute.html> (Stand: 18.08.2013).

⁸⁶³ Vgl ebenso <http://www.fma.gv.at/de/unternehmen/zahlungsinstitute.html> (Stand: 18.08.2013).

⁸⁶⁴ *Lengauer*, Union Aktuell, ZfRV 2008, 148 (148).

⁸⁶⁵ *Sedlak*, Schaffung des europäischen Zahlungsraumes – SEPA und das Zahlungsdienstegesetz, NetV 2010, 7 (8) sowie bereits *Priesemann*, Regulierung und Überwachung im einheitlichen Zahlungsverkehrsmarkt, ÖBA 2006, 855 (855 ff).

Zusätzlich zu den Überweisungen und den unterschiedlichen Formen von Lastschriftverfahren sind auch Kartenzahlungen Teil von SEPA.⁸⁶⁶ Karteninhaber sollen künftig mit ihrer Karte in der Lage sein, SEPA-weit in der gleichen Bequemlichkeit und mit den gleichen Konditionen bargeldlos zahlen (und Bargeldbezüge tätigen) zu können, wie sie dies derzeit in ihrem Heimatland vornehmen.⁸⁶⁷ Zur Erhöhung der Sicherheit sollen alle Karten zusätzlich zum Magnetstreifen mit einem EMV-Chip ausgestattet werden.⁸⁶⁸

⁸⁶⁶ *Judt/Koller*, Innovation im kartengestützten Zahlungsverkehr, ÖBA 2008, 250 (257).

⁸⁶⁷ *Judt/Koller*, Innovation im kartengestützten Zahlungsverkehr, ÖBA 2008, 250 (257).

⁸⁶⁸ Vgl für weitere Details: *Judt/Koller*, Innovation im kartengestützten Zahlungsverkehr, ÖBA 2008, 250 (257).

D. Bankgeheimnis und Datenschutzrecht

1. Verhältnis von Bankgeheimnis und Datenschutzrecht

Maßgebliche Bestimmung ist § 15 Abs 1 DSG. Demnach haben Auftraggeber, Dienstleister und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – „Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, *unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten*, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis)“⁸⁶⁹. Datenschutz und Bankgeheimnis bestehen somit nebeneinander.⁸⁷⁰

In Bezug auf den Informationsaustausch mit ausländischen Finanzbehörden hat Österreich das Bankgeheimnis bisher fortlaufend aufgeweicht.⁸⁷¹

Neben dem Bankgeheimnis und dem Datenschutz ist im Bereich der Finanzdienstleistungen auch § 1 UWG⁸⁷² zu beachten, der allgemein unlautere Geschäftspraktiken oder sonstige unlautere Handlungen zur nicht nur unerheblichen Beeinflussung des Wettbewerbs untersagt, wovon im Einzelfall auch die Offenbarung von Geheimnissen erfasst sein kann.⁸⁷³

Es ist daher jeweils genau zu prüfen, inwieweit die Kreditinstitute zur Offenlegung von Informationen gesetzlich verpflichtet werden können. In Deutschland wurde etwa bereits in den 90er Jahren kritisiert, dass die Banken „von der Steuerfahndung wie eine zu ihren

⁸⁶⁹ § 15 Abs 1 DSG.

⁸⁷⁰ Vgl *Oppitz in Eilmansberger et altera*, Geheimnisschutz, Datenschutz, Informationsschutz, 269 (272 f) mit Verweis auf *Duschanek/Rosenmayr-Klemenz*, DSG 2000, 71; zum deutschen Bankgeheimnis vgl *Nobbe*, Bankgeheimnis, Datenschutz und Abtretung von Darlehensforderungen, WM 2005, 1537 (1538 f) sowie *Hofmann/Walter*, Die Veräußerung Not leidender Kredite – aktives Risikomanagement der Bank im Spannungsverhältnis zwischen Bankgeheimnis und Datenschutz, WM 2004, 1566 (1570 f) und *Rinze/Heda*, Non-Performing Loan und Verbriefungs-Transaktionen: Bankgeheimnis, Datenschutz, § 203 StGB und Abtretung – zugleich eine Besprechung des Urteils des OLG Frankfurt a.M. vom 25. Mai 2004 (= WM 2004, 1386), WM 2004, 1557 (1560 f und 1563).

⁸⁷¹ Vgl *Lafite/Vondrak/Gruber*, Quo vadis Bankgeheimnis? Möglichkeiten und Grenzen bei der Umsetzung des OECD-Standards betreffend Informationsaustausch in Steuersachen, *ecolex* 2009, 573 (576) und *Lafite/Vondrak/Gruber*, Spiel mir das Lied vom Tod, Bankgeheimnis!, *ecolex* 2010, 82 (82 und 85).

⁸⁷² BGBl Nr 448/1984, zuletzt geändert durch BGBl I Nr 112/2013: Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG.

⁸⁷³ Zur vor BGBl I Nr 79/2007 geltenden Rechtslage: *Schobel*, Verletzung von Geheimhaltungspflichten durch Banken, *ÖBA* 2004, 8 (9).

Gunsten eingerichtete Buchführung benutzt“⁸⁷⁴ werden, womit die Ausweitung staatlicher Informationsbefugnisse gegenüber Banken beanstandet wurde.⁸⁷⁵ Auch *Roth/Fitz* wiesen schon 1996 auf die Rolle von Finanzstrafverfahren hin und sprachen in diesem Zusammenhang die Beschränkung des Abgeltungsprinzips der KEST-Regelung auf Steuerinländer an.⁸⁷⁶ Damals wurde zur Verstärkung des Bankgeheimnisses die Herausnahme der Finanzstrafverfahren aus § 38 Abs 2 Z 1 BWG empfohlen,⁸⁷⁷ was heute – soweit ersichtlich – nicht mehr diskutiert wird. Unklarheiten entstehen immer wieder zur Frage, inwieweit das österr Bankgeheimnis auch bei ausländischen Finanzstrafverfahren durchbrochen wird,⁸⁷⁸ besonders in Bezug auf Rechtshilfeersuchen deutscher Finanzbehörden an österr Behörden.⁸⁷⁹

Eine Durchbrechung des Bankgeheimnisses im gerichtlichen oder finanzbehördlichen Strafverfahren (§ 38 Abs 2 Z 1 BWG) ist nur möglich, wenn ein unmittelbarer persönlicher und sachlicher Zusammenhang mit einem bereits eingeleiteten Strafverfahren vorliegt, dadurch sollen reine Erkundungsbeweise nicht möglich sein.⁸⁸⁰

Zu erwähnen ist an dieser Stelle, dass *Apathy* zum Ergebnis gekommen ist, dass sowohl im Schrifttum als auch in der Judikatur die Meinung vorherrsche, dass die Aufzählung der Ausnahmen in § 38 Abs 2 BWG keineswegs taxativ sei.⁸⁸¹ Es wurden somit bereits Durchbrechungen des Bankgeheimnisses anerkannt, welche nicht in § 38 BWG genannt sind.⁸⁸²

2. Exkurs: Abkommen zwischen Österreich und Schweiz

Dass sich die Schweiz gegen den auch in Österreich nach wie vor nicht bestehenden automatischen Informationsaustausch bekennt, wurde bereits 2009 von einem führenden schweizerischen Steuerexperten geäußert.⁸⁸³

⁸⁷⁴ *Meincke*, Geheimhaltungspflichten im Wirtschaftsrecht, WM 1998, 749 (757) mwN.

⁸⁷⁵ Vgl *Meincke*, Geheimhaltungspflichten im Wirtschaftsrecht, WM 1998, 749 (757).

⁸⁷⁶ *Roth/Fitz*, Anonymität, Identitätsfeststellung und Bankgeheimnis, ÖBA 1996, 409 (418 f, 424 und 427).

⁸⁷⁷ *Roth/Fitz*, Anonymität, Identitätsfeststellung und Bankgeheimnis, ÖBA 1996, 409 (424).

⁸⁷⁸ *Urtz*, VwGH-Rechtsprechung: Das österreichische Bankgeheimnis schützt deutsche Steuerstraftäter!, GeS 2007, 21 (22 ff).

⁸⁷⁹ Zur fließenden Grenzziehung zwischen behördlicher und gerichtlicher Amts- oder Rechtshilfe vgl: *Urtz*, VwGH-Rechtsprechung: Das österreichische Bankgeheimnis schützt deutsche Steuerstraftäter!, GeS 2007, 21 (28).

⁸⁸⁰ Vgl *Oppitz* in *Eilmansberger et altera*, Geheimnisschutz, Datenschutz, Informationsschutz, 269 (282).

⁸⁸¹ *Apathy*, Abtretung von Bankforderungen und Bankgeheimnis, ÖBA 2006, 33 (35).

⁸⁸² Vgl *Apathy*, Abtretung von Bankforderungen und Bankgeheimnis, ÖBA 2006, 33 (35 f) mwN.

⁸⁸³ *Frey*, Schweiz schaltet beim Bankgeheimnis jetzt auf hart. Steuerexperte sieht viel Widerstand gegen automatischen Informationsaustausch – Anfragen müssen spezifisch sein, DerStandard 2009/43/01.

Durch das Amtshilfe-Durchführungsgesetz 2009⁸⁸⁴ wurde in Österreich die Verpflichtung für die inländischen Kreditinstitute geschaffen, „aufgrund eines ausländischen Auskunftsamtshilfeersuchens auf der Basis eines dem OECD-Standard entsprechenden DBA oder eines anderen die Amtshilfe regelnden Abkommens die erbetenen Auskünfte zu erteilen bzw der Behörde Einblick in die Unterlagen zu gewähren und diese gegebenenfalls herauszugeben.“⁸⁸⁵ Hierfür sind genau formulierte Feststellungen durch den ersuchenden Staat notwendig, damit das Ersuchen zulässig ist.⁸⁸⁶ Durch dieses Abkommen sind lediglich der Beweisausforschung dienende Maßnahmen („fishing expeditions“) sowie ein Informationsaustausch auf automatischer oder spontaner Basis in Österreich nach wie vor nicht möglich, wengleich Österreich hiermit wesentliche Kriterien für die Streichung von der sog grauen Liste der OECD erfüllt hat.⁸⁸⁷

Im Verhältnis Österreichs zur Schweiz wurde in Bezug auf Besteuerung von „Schwarzgeld“ ein weitergehender Weg beschritten, wengleich der automatische Informationsaustausch nicht durchgeführt werden soll. Unabhängig von konkreten Verdachtsmomenten gegen Österreicher wegen Steuerhinterziehung, sollen schweizerische Kreditinstitute zum Abführen einer einmaligen Pauschalsteuer und jährlicher Zinssteuerbeträgen an Österreich verpflichtet werden. Dadurch erwartet sich Österreich ein zusätzliches Steueraufkommen iHv 1 Mrd € durch die Besteuerung von „Schwarzgeld“ im Jahr 2013 sowie ab dem Jahr 2014 50 Mio € jährlich durch die Besteuerung der Zinserträge.⁸⁸⁸

Das Abkommen wurde mit den Stimmen der SPÖ und ÖVP am 6.7.2012 im Nationalrat beschlossen. Der Bundesrat hat am 19.7.2012 mehrstimmig beschlossen, gegen den Beschluss des NR keinen Einspruch zu erheben und dem Beschluss des Nationalrates gemäß Artikel 50 Absatz 2 Ziffer 2 BVG die verfassungsmäßige Zustimmung zu erteilen.⁸⁸⁹

In der Schweiz sind die „JungsozialistInnen Schweiz“ (JUSO) und die „Aktion für eine unabhängige und neutrale Schweiz“ (AUNS) gegen das Abkommen, welches in ähnlicher

⁸⁸⁴ BGBl I Nr 102/2009: Bundesgesetz über die Umsetzung der OECD-Grundsätze der internationalen abgabenrechtlichen Amtshilfe (Amtshilfe-Durchführungsgesetz – ADG).

⁸⁸⁵ *Jirousek*, Die Umsetzung des OECD-Standards der Amtshilfe in Österreich – das neue Amtshilfe-Durchführungsgesetz, SWI 2009, 488 (488) sowie *Fragner/Schimka*, Finanzausschuss beschließt Initiativantrag zum Amtshilfe-Durchführungsgesetz, GesRZ 2009, 195 (195).

⁸⁸⁶ Vgl *Jirousek*, Die Umsetzung des OECD-Standards der Amtshilfe in Österreich – das neue Amtshilfe-Durchführungsgesetz, SWI 2009, 488 (494) sowie *Gruber/Vondrak*, Initiativantrag zum Amtshilfe-Durchführungsgesetz eingebracht, SWK 2009, T 153 (T 154 f).

⁸⁸⁷ *Jirousek*, Die Umsetzung des OECD-Standards der Amtshilfe in Österreich – das neue Amtshilfe-Durchführungsgesetz, SWI 2009, 488 (494 f).

⁸⁸⁸ Vgl ErläutRV 1770 der Beilagen der XXIV GP, Vorblatt, 5.1. Finanzielle Auswirkungen.

⁸⁸⁹ Vgl http://www.parlament.gv.at/PAKT/VHG/XXIV/BNR/BNR_00585/index.shtml (Stand: 18.08.2013).

Form auch mit Deutschland und Großbritannien geschlossen werden soll.⁸⁹⁰ Die notwendigen Notifikationen gemäß Art 39 Abs 1 des Abkommens wurden am 3.9.2012 bzw am 19.12.2012 vorgenommen; das Abkommen⁸⁹¹ trat somit am 1.1.2013 in Kraft. Die Bestimmungen des Abkommens finden sich in der Anlage zu BGBl III 192/2012. Es wurden zahlreiche – größtenteils gemeinsame – Erklärungen der Vertragsstaaten abgegeben. So erklären die Vertragsstaaten darin etwa, dass die im Abkommen zwischen der Republik Österreich und der Schweizerischen Eidgenossenschaft vereinbarte bilaterale Zusammenarbeit in ihrer Wirkung dem automatischen Informationsaustausch im Bereich der Kapitaleinkünfte dauerhaft gleichkommt.⁸⁹² Die Vertragsparteien werden zudem „die vereinbarten Maßnahmen nach Treu und Glauben durchführen und diese Regelung nicht durch einseitiges Handeln verletzen oder sich im Verhältnis mit Drittparteien gegen diese Regelung wenden.“⁸⁹³

Bedenken hinsichtlich der Gleichheitswidrigkeit konnten von *Beiser*⁸⁹⁴ nachvollziehbar ausgeräumt werden. Er sieht sogar durch die Zusammenarbeit Österreichs und der Schweiz ein gutes Stück mehr Gleichheit und Steuergerechtigkeit im Vergleich zur Ausgangslage vor diesem Abkommen.⁸⁹⁵

Der automatische Informationsaustausch ermöglicht die Verknüpfung zu einer konkreten Person, wohingegen beim Abkommen die Steuer durch das jeweilige Kreditinstitut einbehalten werden soll. ME wäre ein weitergehender Weg sinnvoll. Bei anderen Einkünften abseits der Zinseinkünfte ist eine Offenlegung gegenüber den Finanzbehörden politisch akzeptiert.⁸⁹⁶ Für mich ist nicht nachvollziehbar, weshalb die Zinseinkünfte anders zu behandeln sind. Oft vorgebrachte Argumente, dass damit in die Privatsphäre eingedrungen wird, sind für mich nicht verständlich. Der automatische Informationsaustausch wäre daher auch im Verhältnis zur Schweiz vorzuziehen. Zudem stehen die Bestimmungen des Abkommens im Widerspruch zur aktuellen politischen Position Österreichs, nach der der automatische Informationsaustausch eingeführt werden soll. Die weitere Entwicklung bleibt

⁸⁹⁰ http://diepresse.com/home/wirtschaft/economist/1268226/Schweiz_Volksabstimmung-ueber-Steuerpakt-mit-Wien (Stand: 18.08.2013).

⁸⁹¹ BGBl III 192/2012: Abkommen zwischen der Republik Österreich und der Schweizerischen Eidgenossenschaft über die Zusammenarbeit in den Bereichen Steuern und Finanzmarkt samt Schlussakte einschließlich der dieser beigefügten Erklärungen.

⁸⁹² Vgl Seite 26 des Anhangs zu BGBl III 192/2012.

⁸⁹³ Vgl aaO.

⁸⁹⁴ *Beiser*, Schafft eine Zusammenarbeit zwischen Österreich und der Schweiz mehr Gleichheit?, RdW 2012, 361 (361 ff).

⁸⁹⁵ *Beiser*, Schafft eine Zusammenarbeit zwischen Österreich und der Schweiz mehr Gleichheit?, RdW 2012, 361 (362).

⁸⁹⁶ II.D.2.d) Beginn und Ende des Übergangszeitraumes.

daher abzuwarten. Ich gehe davon aus, dass sich auch die Schweiz in den kommenden Jahren dem automatischen Informationsaustausch anschließen wird.

Nach Informationen des BMF wurden aufgrund des Abkommens aktuell⁸⁹⁷ € 416, Millionen an Österreich überwiesen.⁸⁹⁸ Weitere Beträge sollen jeweils monatlich bis Juni 2014 überwiesen werden.⁸⁹⁹

⁸⁹⁷ Stand: August 2013.

⁸⁹⁸ <https://www.bmf.gv.at/karussell/Steuer.html> (Stand: 18.08.2013).

⁸⁹⁹ Vgl aaO.

E. Reform des „europäischen Datenschutzrechtes“

Gerade im kompetenzrechtlichen Bereich des Datenschutzrechtes gab es immer wieder Entscheidungen des EuGH. So wurden etwa 2006 nach einer Klage des Europäischen Parlaments die Rechtsakte, welche die Übermittlung von Flugpassagierdaten an die USA ermöglichten (Angemessenheitsentscheidung der Europäische Kommission und Beschluss des Rates)⁹⁰⁰, aus kompetenzrechtlichen Gründen für nichtig erklärt.⁹⁰¹

Zur kompetenzrechtlichen Zulässigkeit äußerte sich der EuGH auch jüngst wieder in einem Verfahren, in dem Irland die Vorratsdatenspeicherrichtlinie⁹⁰² nichtig erklären wollte, weil diese auf Art 95 EGV (ehemals sog „erste Säule“) gestützt sei.⁹⁰³ Der EuGH sah die Zweckbestimmung der RL zwar in engem Zusammenhang mit der „polizeilichen und justiziellen Zusammenarbeit in Strafsachen“ (ehemals sog „dritte Säule“), betonte aber, dass die Bestimmungen der RL lediglich die Angleichung der nationalen Rechtsvorschriften in Bezug auf die Vorratsdatenspeicherungspflicht, die Kategorien von auf Vorrat zu speichernden Daten, die Speicherungsfristen, den Datenschutz und die Datensicherheit sowie die Anforderungen an die Vorratsdatenspeicherung bezwecken.⁹⁰⁴ Die RL harmonisiere aber weder die Frage des Zugangs zu den Daten durch die zuständigen nationalen Strafverfolgungsbehörden noch die Frage der Verwendung und des Austauschs dieser Daten zwischen diesen Behörden und wage sich somit nicht in den heiklen Bereich des Zugriffs auf die gespeicherten Daten durch die Behörden.⁹⁰⁵ Art 95 EGV sei daher die zutreffende kompetenzrechtliche Grundlage für die RL zur Vorratsdatenspeicherung.

⁹⁰⁰ 2004/535/EG: Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden (= ABI L 235 vom 6.7.2004, S 11-22) sowie 2004/496/EG: Beschluss des Rates vom 17. Mai 2004 über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security - PNR (Passenger Name Record) (= ABI L 183 vom 20.5.2004, S 83-83).

⁹⁰¹ Vgl *Keiler/Kristoferitsch*, Passagierdaten auf dem Flug in die USA. Neues Abkommen der EU mit den USA über die Weitergabe von Passagierdaten nach dem Urteil des EuGH verbundene Rs C-317/04, C-318/04, ZVR 2006, 484 (484 ff).

⁹⁰² Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (= ABI L 105 vom 13.4.2006, S 54-63).

⁹⁰³ *Barbist*, EuGH zur Vorratsdatenspeicherung - Das Urteil in der Rechtssache Irland gegen Europäisches Parlament/Rat der Europäischen Union, MR 2009, 3 (3).

⁹⁰⁴ *Barbist*, EuGH zur Vorratsdatenspeicherung - Das Urteil in der Rechtssache Irland gegen Europäisches Parlament/Rat der Europäischen Union, MR 2009, 3 (4).

⁹⁰⁵ Vgl ebenso *Barbist*, EuGH zur Vorratsdatenspeicherung - Das Urteil in der Rechtssache Irland gegen Europäisches Parlament/Rat der Europäischen Union, MR 2009, 3 (4).

Um mehr Klarheit zu schaffen, wurden durch den Vertrag von Lissabon auch Kompetenzbestimmungen zur Erlassung von datenschutzrechtlichen Bestimmungen geändert. Ein nun unterbreiteter Vorschlag für eine Datenschutz-Grundverordnung soll zur Einheitlichkeit nationaler datenschutzrechtlicher Normen führen.

Folgende wesentlichen Änderungen werde ich in meiner Arbeit besprechen:

- Änderungen durch den EUV⁹⁰⁶ und den AEUV⁹⁰⁷,
- Vorschlag für eine Datenschutz-Grundverordnung und der
- Vorschlag für eine RL zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

1) Änderungen durch den EUV und den AEUV:

In der konsolidierten Fassung des Vertrags zur Gründung der Europäischen Gemeinschaft,⁹⁰⁸ der nunmehr nicht mehr anwendbar ist, normierte Art 286 EGV, dass ab 1. Januar 1999 die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch diesen Vertrag oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung finden.

Auch die Schaffung einer unabhängigen Kontrollinstanz wurde in Art 286 EGV vorgesehen.⁹⁰⁹

Diese beiden Regelungsinhalte (Anwendung datenschutzrechtlicher Bestimmungen auf die Organe und Einrichtungen der Gemeinschaft sowie die Schaffung einer unabhängigen Kontrollinstanz) wurden in Art 16 Abs 2 AEUV⁹¹⁰ übernommen, wobei die Gesetzgebungskompetenz des Europäischen Parlaments in diesem Bereich geschaffen wurde: Nun erlassen das Europäische Parlament und der Rat gemeinsam „Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und

⁹⁰⁶ Konsolidierte Fassung des Vertrags über die Europäische Union (= ABl C 83 vom 30. März 2010, S 13-46).

⁹⁰⁷ Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union (= ABl C 83 vom 30. März 2010, S 47-200).

⁹⁰⁸ ABl C 325 vom 24. Dezember 2002, 33-184.

⁹⁰⁹ Vgl Art 286 Abs 2 EGV.

⁹¹⁰ Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union (= ABl C 83 vom 30. März 2010, S 47-200).

über den freien Datenverkehr.“⁹¹¹ Gem Satz 2 leg cit wird die Einhaltung dieser Vorschriften von unabhängigen Behörden überwacht.

Wortgleich mit Art 8 der Charta der Grundrechte der Europäischen Union⁹¹² normiert Art 16 Abs 1 AEUV, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat.

Sofern eine sekundärrechtliche Regelung nicht auf Art 16 AEUV gestützt werden kann, bleibt daher Art 114 AEUV (ex-Art 95 EGV) weiterhin zu beachten. Art 114 AEUV ermöglicht die Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.⁹¹³ Gestützt auf die Vorgängerbestimmung (Art 95 EGV) wurde die Datenschutz-Richtlinie erlassen.

Der in Art 16 Abs 2 letzter Satz AEUV zu findende Verweis auf Art 39 EUV als *lex specialis* erschließt sich erst bei genauerer Recherche: Für den Bereich des 2. Kapitels des V. Titels EUV namens „Besondere Bestimmungen über die Gemeinsame Aussen- und Sicherheitspolitik“⁹¹⁴ wird eine zu Art 16 Abs 2 AEUV abweichende Regelung getroffen. Demnach erlässt der Rat einen Beschluss zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von in den Anwendungsbereich des 2. Kapitels EUV fallender Tätigkeiten und über den freien Datenverkehr. Auch hier wird normiert, dass die Einhaltung dieser Vorschriften von unabhängigen Behörden überwacht wird.⁹¹⁵

Im Ergebnis besteht somit im Bereich der GASP das Einstimmigkeitserfordernis im Rat. Vor allem aber hat das Europäische Parlament keine Mitbestimmungsbefugnis.⁹¹⁶ Art 39 EUV wird mit Blick auf Art 24 Abs 1 Unterabsatz 2 Satz 3 EUV verständlich, der den Erlass von Gesetzgebungsakten im Bereich der GASP ausschließt.⁹¹⁷ Als Vorgängerbestimmung wird Art 286 EGV betrachtet, welcher die Datenschutz-RL, welche sich an die einzelnen Mitgliedstaaten richtete, für die Gemeinschaft selbst verbindlich erklärte.⁹¹⁸ Es besteht somit

⁹¹¹ Art 16 Abs 2 erster Satz AEUV.

⁹¹² Vgl VI.A.3 Charta der Grundrechte der Europäischen Union.

⁹¹³ Vgl Art 114 Abs 1 AEUV.

⁹¹⁴ Vgl Überschrift zu Art 23 EUV.

⁹¹⁵ Art 39 letzter Satz EUV.

⁹¹⁶ *Ennöckl*, EuGH zur Veröffentlichung von EU-Agrarbeihilfen: (vorläufiges) Ende der Transparenz, ÖJZ 2011, 955 (956, FN 9) mit Verweis auf *Zerdick* in *Lenz/Borchardt* (Hrsg), EU-Verträge⁵ Art 16 AEUV Rz 10. Vgl auch *Zerdick* in *Lenz/Borchardt* (Hrsg), EU-Verträge⁵ Art 16 AEUV Rz 30.

⁹¹⁷ Vgl *Funke*, Umsetzungsrecht, 312. *Funke* verweist jedoch fälschlicherweise auf Art 23 EUV samt Absätzen, wobei Art 23 EUV nicht in Absätze unterteilt ist.

⁹¹⁸ Zur Bindungswirkung von Art 39 EUV: *Funke*, Umsetzungsrecht, 312 f mwN.

im Bereich des Datenschutzrechtes der gemeinsamen Aussen- und Sicherheitspolitik kein Mitspracherecht des Europäischen Parlaments. ME wäre aus demokratischer Sicht eine Einbindung des Europäischen Parlaments in diesem Gebiet sinnvoll und würde zur Entwicklung einer demokratisch orientierten Wertegemeinschaft und zur Einheitlichkeit innerhalb der Europäischen Union wesentlich beitragen.

2) Vorschlag für eine Datenschutz-Grundverordnung:

Im Jänner 2012 wurde von der Kommission ein Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) präsentiert.⁹¹⁹ Dieser Verordnungsentwurf soll sowohl eine Aktualisierung und Anpassung des bestehenden europäischen Datenschutzrechts an moderne Formen der Datenverarbeitung bewirken (Stichwort: Soziale Netzwerke), als auch eine Harmonisierung des europäischen Datenschutzrechts herbeiführen, damit die Wettbewerbsfähigkeit des europäischen Binnenmarkts gesteigert werden kann.⁹²⁰

Wesentliche Änderungen im Verordnungsentwurf sind:⁹²¹

- Einführung der Datenbegriffe „genetische Daten“ und „biometrische Daten“,
- Juristische Personen sollen national nicht mehr von Datenschutzregelungen erfasst werden – Schutz von natürlichen Personen wird anerkannt,⁹²²
- „Privacy by Default“ - Ansatz – personenbezogene Daten sollen nur im absolut notwendigen Ausmaß verarbeitet werden,
- Erweiterung der Betroffenenrechte (zB „data breach notification duty“ – Meldepflicht bei Verletzungen des Schutzes von personenbezogenen Daten, nur noch explizite Zustimmung für Datenverwendungen, „Recht auf Vergessen“, „Recht auf Datenübertragbarkeit“, Widerspruchsrecht gegen Profiling),⁹²³
- Geldstrafen sollen bis zu EUR 1 Million oder 2 % des weltweiten Jahresumsatzes eines Unternehmens betragen,⁹²⁴
- Datenschutzbehörden der Hauptniederlassung sollen bei Beschwerden zuständig sein („One-Stop-Shop“),⁹²⁵

⁹¹⁹ Vorschlag vom 25.01.2012, KOM/2012/11 endg (COD).

⁹²⁰ Vgl *Leissler*, Der neue europäische Datenschutzrahmen, *ecolex* 2012, 268 (268).

⁹²¹ Vgl im Folgenden: *Leissler*, Der neue europäische Datenschutzrahmen, *ecolex* 2012, 268 (268 f).

⁹²² Vgl auch *Knyrim*, *Datenschutzrecht*², IX.

⁹²³ Vgl weitere Details: *Knyrim*, *Datenschutzrecht*², IX f, der jedoch den Verordnungsentwurf aufgrund der zeitlichen Distanz zur Erscheinung des Buches nur umreißen konnte.

⁹²⁴ *Knyrim*, *Datenschutzrecht*², IX.

⁹²⁵ *Knyrim*, *Datenschutzrecht*², X.

- Datenschutzbeauftragte werden (erst ab 250 Mitarbeitern) geschaffen,⁹²⁶ wobei dieser in der Hauptniederlassung angesiedelt sein soll,
- Regelungen über „gemeinsam für die Verarbeitung Verantwortliche“ (vgl Informationsverbundsystem) werden geschaffen, wobei die Verantwortlichen gesamtschuldnerisch für die Schäden haften⁹²⁷ sowie
- Erweiterung der Prinzipien des internationalen Datenverkehrs durch Aufnahme des Modells der sog „Binding Corporate Rules“.⁹²⁸

Der Verordnungsentwurf soll, nach Prognose von Optimisten, bis Ende 2012/Anfang 2013 den europäischen Rat und das europäische Parlament passiert haben und dann zwei Jahre nach der Veröffentlichung im ABl in Kraft treten, weshalb damit dzt frühestens Ende 2014/Anfang 2015 zu rechnen ist.⁹²⁹

Durch die wesentlich erhöhten Strafbestimmungen und die unionsweit einheitlichen Regelungen soll die Bedeutung des Datenschutzrechtes in den Unternehmen gesteigert werden und somit der Schutz der personenbezogenen Daten verbessert werden. Abzuwarten bleibt, inwiefern die erforderlichen Quoren (grundsätzlich qualifiziertes Quorum im Rat und einfache Mehrheit im Europäischen Parlament)⁹³⁰ erfüllbar sind.

3) Vorschlag für eine RL zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich der PJZS:

Zur Stärkung der Binnenmarktdimension beim Datenschutz, zur wirksameren Ausübung der Datenschutzrechte durch den Einzelnen und zur Schaffung einer umfassenden, kohärenten Regelung für alle Zuständigkeitsbereiche der Union einschließlich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS)⁹³¹ gehört neben der Datenschutz-Grundverordnung auch der ebenfalls 2012 präsentierte Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der

⁹²⁶ Kritisch dazu: *Knyrim*, Datenschutzrecht², IX.

⁹²⁷ Ebenso: *Knyrim*, Datenschutzrecht², IX.

⁹²⁸ *Knyrim*, Datenschutzrecht², X.

⁹²⁹ Vgl *Knyrim*, Datenschutzrecht², XI.

⁹³⁰ *Zerdtick* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Art 16 AEUV Rz 29 mit Verweis auf das ordentliche Gesetzgebungsverfahren nach Art 294 AEUV (vgl *Hetmeier* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Art 294 AEUV Rz 1 ff.

⁹³¹ Vgl KOM (2012) 10 endg, S 4.

Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.⁹³²

Gestützt auf Art 16 Abs 2 AEUV können Vorschriften über den Schutz natürlicher Personen bei der grenzübergreifenden sowie der innerstaatlichen Verarbeitung personenbezogener Daten auch für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erlassen werden. Die Besonderheit der polizeilichen und justiziellen Zusammenarbeit in Strafsachen rechtfertigen, dass spezifische Vorschriften für den Schutz personenbezogener Daten und den freien Verkehr derartiger Daten in diesem Bereich erlassen werden können.⁹³³

Diese Regelung soll den Rahmenbeschluss 2008/977/JI des Rates⁹³⁴ ersetzen.⁹³⁵

Der Rahmenbeschluss (RB) 2008/977/JI wurde größtenteils vor dessen Erlassung im DSG bereits umgesetzt, wobei das im RB vorgesehene Auskunftsrecht in Österreich unzureichend umgesetzt wurde.⁹³⁶

In Österreich gilt das DSG auch für den Bereich der Justiz und Polizei, wenngleich auch Spezialgesetze⁹³⁷ bestehen. Meiner Meinung nach wäre es wertvoll, sich in einer separaten wissenschaftlichen Arbeit mit dem Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit auseinander zu setzen.

⁹³² KOM (2012) 10 endg.

⁹³³ Vgl KOM (2012) 10 endg, S 2.

⁹³⁴ Vgl V.B.5 Weitere zu beachtende Vorschriften und Mitteilungen V.B.5.

⁹³⁵ Vgl Art 58 des RL-Vorschlages.

⁹³⁶ Vgl Stellungnahme des Datenschutzzrates in seiner 190. Sitzung vom 9. Oktober 2009 zum Bundesgesetz, mit dem ein Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol) erlassen wird sowie das Polizeikooperationsgesetz und das Sicherheitspolizeigesetz geändert werden (8/SN-90/ME), S 6.

⁹³⁷ Vgl etwa das Sicherheitspolizeigesetz und das EU-Polizeikooperationsgesetz.

VI. Grundrechtliche Analyse

Im letzten Kapitel vor den Schlussfolgerungen meiner Arbeit werde ich mich mit der grundrechtlichen Perspektive des Datenschutzes auseinandersetzen. Nach einer Darstellung der österreichischen und europäischen Normen und deren Zusammenhänge⁹³⁸ werde ich noch kurz auf technische Aspekte des Datenschutzes⁹³⁹ eingehen.

A. Grundrecht auf Datenschutz

Zentrale Norm zum Grundrecht auf Datenschutz ist § 1 DSG, der so wie der gesamte Artikel 1 (§§ 1 bis 3 DSG) des DSG und bestimmte andere Normen des DSG⁹⁴⁰ eine Verfassungsbestimmung ist. Zudem sind die Charta der Grundrechte der Europäischen Union⁹⁴¹ und die Europäische Menschenrechtskonvention⁹⁴² zu beachten, wobei die von diesen Bestimmungen gedeckten Schutzbereiche keinesfalls gleich sind, aber durchaus gemeinsame Schutzbereiche haben. Auf deren Verhältnis zueinander werde ich an späterer Stelle genauer eingehen.

1. § 1 DSG

Das Grundrecht auf Datenschutz in § 1 DSG ist auf folgende Weise normiert:⁹⁴³

§ 1 Abs 1 DSG bestimmt, dass „jedermann“, womit natürliche und juristische Personen gemeint sind,⁹⁴⁴ Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit daran ein schutzwürdiges Interesse besteht. Insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens besteht dieser Geheimhaltungsanspruch.⁹⁴⁵ Das schutzwürdige Interesse ist *expressis verbis* ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind. Darunter werden rechtlich frei zugängliche („allgemein verfügbar“) sowie anonyme („mangelnde Rückführbarkeit auf den Betroffenen“) Daten subsumiert.

⁹³⁸ Vgl VI.A Grundrecht auf Datenschutz.

⁹³⁹ Vgl VI.B Datenschutz und Technik.

⁹⁴⁰ Vgl § 35 Abs 2 DSG (Kontrolle der DSK auch über die in Art 19 B-VG bezeichneten obersten Organe der Vollziehung), § 38 Abs 1 DSG (Organisation und Geschäftsführung der DSK) und § 61 Abs 4 DSG (Übergangsbestimmung).

⁹⁴¹ Konsolidierte Fassung der Charta der Grundrechte der Europäischen Union (= ABl C 83 vom 30.03.2010, S 389-403).

⁹⁴² BGBl Nr 210/1958, zuletzt geändert durch BGBl III Nr 47/2010: Konvention zum Schutze der Menschenrechte und Grundfreiheiten.

⁹⁴³ Vgl § 1 DSG.

⁹⁴⁴ Lehner in Heissl (Hg), Handbuch Menschenrechte (2009) Rz 11/8, S 213.

⁹⁴⁵ Vgl § 1 Abs 1 erster Satz DSG.

Abs 2 leg cit normiert, in welchen Fällen die Verwendung der vom Schutzbereich erfassten personenbezogenen Daten zulässig ist. Es werden drei Gruppen unterschieden:

- Verwendung personenbezogener Daten im lebenswichtigen Interesse des Betroffenen,
- Zustimmung des Betroffenen zur Verwendung seiner personenbezogener Daten und
- Verwendung der Daten zur Wahrung überwiegend berechtigter Interessen eines anderen.

Die Verwendung im lebenswichtigen Interesse des Betroffenen ist nur dann zulässig, wenn eine Zustimmung des Betroffenen nicht rechtzeitig eingeholt werden kann.⁹⁴⁶

Was die unterschiedlichen Formen der Zustimmung im DSGVO betrifft, werde ich auf die dazu bereits ausführlich bestehende Literatur verweisen.⁹⁴⁷ Die große Bedeutung der datenschutzrechtlichen Zustimmung in der Praxis wurde ebenso schon umfassend behandelt.⁹⁴⁸ Um die bestehenden einfachgesetzlichen Bestimmungen⁹⁴⁹ verfassungskonform interpretieren zu können ist meiner Meinung nach notwendig, dass die vom Betroffenen erteilte Zustimmung ohne jegliche Zweifel als Zustimmung zu werten ist und dass diese von ihm frei erteilt wurde. Dazu ist eine ausreichende Information über den konkreten Sachverhalt erforderlich.

Am meisten Unklarheit kann mE im dritten Bereich der Zulässigkeit der Verwendung der Daten entstehen, zumal die Ziehung scharfer Grenzen in diesem Bereich sehr schwierig ist. So spielt sich die Frage der Lebensbedrohlichkeit, oder ob eine Zustimmung gegeben wurde, in einem relativ engen Bereich ab. Ob jedoch die Interessen eines anderen zur Verwendung der Daten überwiegen, ist jeweils ein Ergebnis einer langen Abwägung der einzelnen bestehenden Interessen.⁹⁵⁰

Hierfür bietet § 1 DSGVO gewisse Hilfestellungen zur Abwägung, wobei der Eingriff jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf.⁹⁵¹

⁹⁴⁶ Vgl zu den einfachgesetzlichen Bestimmungen im DSGVO und der Datenschutz-RL: *Duschanek*, § 1 DSGVO 2000, Rz 45, S 36 f.

⁹⁴⁷ Vor allem *Duschanek*, § 1 DSGVO 2000, Rz 46 f, S 37 ff sowie *Jahnel*, Handbuch Datenschutzrecht, 3/130 ff.

⁹⁴⁸ *Reimer* in *Jahnel/Siegrwart/Fercher (Hg)*, Aktuelle Fragen des Datenschutzrechtes, 185 ff.

⁹⁴⁹ Insb §§ 4 Z 14, 8 Abs 1 Z 2, 9 Z 6 und 12 Abs 3 Z 5 DSGVO.

⁹⁵⁰ Vgl auch *Reimer* in *Jahnel/Siegrwart/Fercher (Hg)*, Aktuelle Fragen des Datenschutzrechtes, 186 f.

⁹⁵¹ Vgl § 1 Abs 2 letzter Satz DSGVO.

§ 1 Abs 2 DSGVO sieht bei „Eingriffen einer staatlichen Behörde“ vor, dass diese nur auf Grund von Gesetzen zulässig sind und nennt hierfür weitere besondere Voraussetzungen (va Notwendigkeit iSd Art 8 Abs 2 EMRK). Wesentlich für das Verständnis ist daher, was unter einer „staatlichen Behörde“ zu verstehen ist. *Duschanek*⁹⁵² verweist hierbei auf *Raschauer*⁹⁵³, der „Behörde (Gericht oder Verwaltungsbehörde)“ als Teilmenge des Begriffs „Organ“ sieht. Demnach sind unter Behörden jene Organe zu verstehen, denen hoheitliche Aufgaben übertragen sind, „insb wenn sie zur Erlassung von Bescheiden oder Verordnungen oder zur Setzung von AuvBZ berufen sind.“⁹⁵⁴ Entscheidend ist daher die konkrete Ermächtigung aus den materiell-rechtlichen Verwaltungsvorschriften, weshalb es keine Behörde im organisatorischen Sinn, sondern ausschließlich Behörden im funktionellen Sinn gibt.⁹⁵⁵ Erfasst sind somit auch die „schlichte Hoheitsverwaltung“⁹⁵⁶ sowie Fälle der Ausstattung Privater mit hoheitlichen Befugnissen.⁹⁵⁷

Folgende Voraussetzungen müssen bei „behördlichen Eingriffen“ erfüllt werden, wobei stets überwiegend berechtigte Interessen für den behördlichen Eingriff vorzuliegen haben:

- Gesetze, die aus den in Art 8 Abs 2 der EMRK genannten Gründen notwendig sind, müssen für den Eingriff bestehen.⁹⁵⁸
- Bei besonders schutzwürdigen Daten dürfen die Gesetze die Verwendung der Daten nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen.

Jüngst sorgte die Aufforderung der Finanzmarktaufsicht (FMA) an etwa 30 Wertpapierdienstleister (WPDL) für Aufregung:⁹⁵⁹ Die WPDL wurden Anfang April 2009 per Bescheid aufgefordert, der FMA „binnen sieben Tagen von sämtlichen, höchstens jedoch 1.000, Kunden die folgenden Daten zu übermitteln: Name, Adresse, Geburtsdatum, Anlagevolumen, Beginn des Kundenverhältnisses sowie die Bezeichnung des zuständigen

⁹⁵² Vgl *Duschanek*, § 1 DSGVO 2000, Rz 52, S 42 f.

⁹⁵³ *Raschauer*, Allgemeines Verwaltungsrecht³, Rz 138.

⁹⁵⁴ *Raschauer*, Allgemeines Verwaltungsrecht³, Rz 138.

⁹⁵⁵ Vgl *Raschauer*, Allgemeines Verwaltungsrecht³, Rz 138.

⁹⁵⁶ Vgl *Duschanek*, § 1 DSGVO 2000, Rz 52, S 42 f. mit Verweis auf *Raschauer*, Allgemeines Verwaltungsrecht³, Rz 700 f, wonach der Kontext des Handelns für die normative Qualität des Aktes von Bedeutung ist (genannt werden aaO etwa eine Auskunft im Rahmen eines behördlichen Verfahrens oder die [tatsächliche] Auszahlung einer bescheidförmig zuerkannten Summe Geldes).

⁹⁵⁷ Vgl im Detail: *Duschanek*, § 1 DSGVO 2000, Rz 52 ff, S 42 ff.

⁹⁵⁸ Auf Art 8 Abs 2 EMRK werde ich noch weiter unten genauer eingehen: Vgl VI.A.2 Europäische Menschenrechtskonvention.

⁹⁵⁹ Vgl *Brandl/Knoll*, Datenschutzrechtliche Grenzen der FMA-Prüfung, *ecolex* 2009, 443 (443 ff).

Beraters (<Stammdaten-Liste>).⁹⁶⁰ Die eingehende Prüfung durch *Brandl/Knoll* zeigte, dass auch die FMA an die Bestimmungen des DSG gebunden ist⁹⁶¹ und die Vorgehensweise der FMA im konkreten Fall dem DSG widerspricht.⁹⁶² Den WPDL stand somit die Möglichkeit zur Verfügung, sich gegen den Bescheid mittels Beschwerde an den VfGH und/oder VwGH zur Wehr zu setzen.⁹⁶³ Eine Beschwerde beim VfGH hätte dann Erfolg, wenn sie auf den Vorwurf der Gesetzlosigkeit, der denkbaren Gesetzesanwendung oder der Anwendung eines verfassungswidrigen Gesetzes gestützt wird,⁹⁶⁴ da der VfGH nur eine „Grobprüfung“ nach Maßgabe des garantierten Inhaltskerns der in § 1 DSG formulierten Ansprüche vornimmt.⁹⁶⁵

Der VfGH erkannte im konkreten Fall, dass der Eingriff nur zulässig sei, „wenn das zu seiner Rechtfertigung herangezogene Interesse die schutzwürdigen Interessen sämtlicher Betroffenen überwiegt.“⁹⁶⁶ Die Geeignetheit und die Verhältnismäßigkeit der Aufforderungen im Bescheid der FMA an den WPDL wurde vom VfGH verneint, weshalb der angefochtene Bescheid die beschwerdeführende Gesellschaft in ihrem verfassungsgesetzlich gewährleisteten Grundrecht auf Datenschutz gemäß §1 DSG verletzt hat und daher aufzuheben war.⁹⁶⁷

Ergänzend sei nur erwähnt, dass im Bereich der Vorfeldermittlungen im Strafrecht manche Autoren vom öffentlichen Niedergang der Grundsätze des Datenschutzes sprechen.⁹⁶⁸ Kritisch äußerte sich auch *Hackl* zum Standard Audit File – Tax (SAF-T), wodurch Daten auf Datenträgern im xml-Format der Finanzverwaltung zur Verfügung gestellt werden können.⁹⁶⁹

Durch den gesteigerten Schutz für „besonders schutzwürdige Daten“ soll nach den Vorgaben der Datenschutz-Richtlinie der Schutz sensibler Daten sichergestellt werden.⁹⁷⁰ Auffällig ist, dass verfassungsrechtlich nur vorgeschrieben wird, dass bei privaten Eingriffen in das Geheimhaltungsrecht Betroffener das Interesse des Privaten überwiegen muss. Bei der

⁹⁶⁰ *Brandl/Knoll*, Datenschutzrechtliche Grenzen der FMA-Prüfung, *ecolex* 2009, 443 (443).

⁹⁶¹ *Brandl/Knoll*, Datenschutzrechtliche Grenzen der FMA-Prüfung, *ecolex* 2009, 443 (444).

⁹⁶² *Brandl/Knoll*, Datenschutzrechtliche Grenzen der FMA-Prüfung, *ecolex* 2009, 443 (446).

⁹⁶³ *Brandl/Knoll*, Datenschutzrechtliche Grenzen der FMA-Prüfung, *ecolex* 2009, 443 (446).

⁹⁶⁴ *Duschaneck*, § 1 DSG 2000, Rz 90, S 73 zur Verletzung des Grundrechts durch einen Bescheid der DSK.

⁹⁶⁵ Vgl *Duschaneck*, § 1 DSG 2000, Rz 74, S 61.

⁹⁶⁶ VfGH 17.12.2009, B 504/09, unter „IV. 1.“.

⁹⁶⁷ Vgl VfGH 17.12.2009, B 504/09, unter „IV. 2. und 3.“.

⁹⁶⁸ *Hassemer*, Strafrecht im Wandel, JRP 2007, 79 (84).

⁹⁶⁹ *Hackl*, Der „gläserne Unternehmer“, SWK 2009, T 63 (T 66).

⁹⁷⁰ Vgl *Walter/Mayer/Kucsko-Stadlymayer*, Verfassungsrecht¹⁰ Rz 1444, S 713 sowie *Öhlinger*, Verfassungsrecht⁸ Rz 830.

Interpretation dieser Bestimmung sind somit die Bestimmungen der DSRL bzw die in Österreich erfolgte Umsetzung der DSRL im DSG zu beachten.

Bei der Betrachtung des § 1 DSG fällt zudem auf, dass in Abs 3 leg cit mehrere subjektive Rechte explizit genannt werden. Demnach hat jedermann, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen⁹⁷¹ folgende Rechte:

- 1) Recht auf Auskunft,
- 2) Recht auf Richtigstellung unrichtiger Daten,
- 3) Recht auf Löschung unzulässigerweise verarbeiteter Daten.⁹⁷²

Beschränkungen dieser Rechte des § 1 Abs 3 DSG sind nur zulässig, wenn die in § 1 Abs 2 DSG genannten Voraussetzungen erfüllt werden.

Die in § 1 Abs 3 DSG genannten Rechte stellen eine Anspruchsgrundlage dar, deren Rechtsdurchsetzung gerade bei den hoheitlichen Realakten der Löschung oder der Richtigstellung nicht immer zweifelsfrei geklärt ist.⁹⁷³ Im öffentlichen Bereich kann sich der Betroffene an die DSK wenden, die dann mit Bescheid entscheidet, wobei gem § 40 Abs 4 DSG der Auftraggeber des öffentlichen Bereichs verpflichtet ist, „unverzüglich den der Rechtsanschauung der DSK entsprechenden Zustand herzustellen.“⁹⁷⁴

§ 1 Abs 5 DSG normiert, dass das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind und soweit sie nicht in Vollziehung der Gesetze tätig werden, auf dem Zivilrechtsweg geltend zu machen ist. Damit wird eine unmittelbare Drittwirkung des Grundrechtes auf Datenschutz ausdrücklich normiert.⁹⁷⁵ Sofern nicht Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind, ist in allen übrigen Fällen im öffentlichen Bereich die DSK zur Entscheidung zuständig.⁹⁷⁶

⁹⁷¹ Hiermit wird auf (einfach)gesetzliche Ausführungsbestimmungen, die vor allem im DSG zu finden sind, verwiesen.

⁹⁷² Dieses Recht wird in § 1 Abs 3 Z 2 genannt, ist jedoch als separates Recht zu nennen, da es neben dem Recht auf Richtigstellung besteht und auch unabhängig von diesem Recht durchgesetzt werden kann.

⁹⁷³ Vgl *Raschauer* in *Holoubek/Lang (Hg)*, Rechtsschutz gegen staatliche Untätigkeit, 277.

⁹⁷⁴ § 40 Abs 4 DSG sowie *Raschauer* in *Holoubek/Lang (Hg)*, Rechtsschutz gegen staatliche Untätigkeit, 277.

⁹⁷⁵ *Walter/Mayer/Kucsko-Stadlymayer*, Verfassungsrecht¹⁰ Rz 1441, S 711 sowie *Wiederin*, Schutz der Privatsphäre, in: *Merten/Papier*, HGR VII/1, § 190 Rz 24 mwN.

⁹⁷⁶ Vgl § 1 Abs 5 DSG letzter Satz.

Das Datenschutzgesetz räumt somit den Betroffenen auch gegenüber Privatpersonen einen Anspruch auf Achtung des Geheimhaltungsinteresses an personenbezogenen Daten ein. Diese legislative Festsetzung der unmittelbaren Drittwirkung auf Verfassungsebene ist im Vergleich zu anderen Grundrechten einzigartig und von besonderer Bedeutung.⁹⁷⁷ Das Grundrecht auf Datenschutz gilt unabhängig davon, ob personenbezogene Daten in automationsunterstützter Form oder manuell verarbeitet werden.⁹⁷⁸

Eine bedeutsame Änderung erfolgte im Rahmen der Verwaltungsgerichtsbarkeits-Novelle 2012:⁹⁷⁹ § 1 Abs 5 DSG, sowie weitere Bestimmungen, die im Zusammenhang mit der DSK stehen,⁹⁸⁰ wurden aufgehoben. Diese Normen treten gem Art 2 Abs 2 des BGBl I 51/2012 mit 31.12.2013 außer Kraft. Durch die Verwaltungsgerichtsbarkeits-Novelle soll entsprechend dem Regierungsprogramm der Bundesregierung für die XXIV. Gesetzgebungsperiode eine mehrstufige Verwaltungsgerichtsbarkeit geschaffen werden, wodurch ein Ausbau des Rechtsschutzsystems im Sinne einer Verfahrensbeschleunigung und eines verstärkten Bürgerservice, als auch die Entlastung des Verwaltungsgerichtshofes erreicht werden soll.⁹⁸¹ So wird auch die DSK in der bestehenden Form abgeschafft werden.⁹⁸² Die Zuständigkeiten der Kollegialbehörden mit richterlichem Einschlag sowie der sonstigen weisungsfrei gestellten Organe sollen betreffend die rechtsprechende Tätigkeit auf die Verwaltungsgerichte übergehen.⁹⁸³

2. Europäische Menschenrechtskonvention

Artikel 8 der Europäischen Menschenrechtskonvention⁹⁸⁴ trägt die Überschrift „Recht auf Achtung des Privat- und Familienlebens“ und lautet:

⁹⁷⁷ *Walter/Mayer/Kucsko-Stadlymayer*, Verfassungsrecht¹⁰ Rz 1336, S 627; vgl auch *Kunnert*, Das „gläserne Auto“ – Überlegungen aus datenschutzrechtlicher Sicht, ZVR 2002, 219 (219 f) sowie *Öhlinger*, Verfassungsrecht⁸ Rz 742.

⁹⁷⁸ *Kunnert*, Das „gläserne Auto“ – Überlegungen aus datenschutzrechtlicher Sicht, ZVR 2002, 219 (219 f) mit Verweis auf § 1 Abs 3 DSG.

⁹⁷⁹ BGBl I Nr 51/2012: Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Finanz-Verfassungsgesetz 1948, das Finanzstrafgesetz, das Bundesgesetz, mit dem das Invalideneinstellungsgesetz 1969 geändert wird, das Bundessozialamtsgesetz, das Umweltverträglichkeitsprüfungsgesetz 2000, das Bundesgesetzblattgesetz, das Verwaltungsgerichtshofgesetz 1985 und das Verfassungsgerichtshofgesetz 1953 geändert und einige Bundesverfassungsgesetze und in einfachen Bundesgesetzen enthaltene Verfassungsbestimmungen aufgehoben werden (Verwaltungsgerichtsbarkeits-Novelle 2012).

⁹⁸⁰ Genannt werden in Art 2 Abs 1 Z 9 der Verwaltungsgerichtsbarkeits-Novelle 2012 folgende Bestimmungen: § 1 Abs 5, § 35 Abs 2 und § 38 Abs 1 DSG.

⁹⁸¹ Vorblatt zur ErläutRV 1618 der XXIV GP.

⁹⁸² Vgl Art 1 Z 85 des BGBl I Nr 51/2012, wonach auf Art 152 B-VG die Anlage „Aufgelöste unabhängige Verwaltungsbehörden“ folgt mit dem unter „A. Bund“ zu findenden Punkt „25. Datenschutzkommission“.

⁹⁸³ ErläutRV 1618 der XXIV GP, Allgemeiner Teil – Hauptgesichtspunkte des Entwurfes.

⁹⁸⁴ BGBl Nr 210/1958, zuletzt geändert durch BGBl III Nr 47/2010: Konvention zum Schutze der Menschenrechte und Grundfreiheiten.

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Die Europäische Menschenrechtskonvention ist gemäß BVG⁹⁸⁵ in Österreich mit Verfassungsrang ausgestattet.

Der Vertrag über die Europäische Union sieht „die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, (...) als allgemeine Grundsätze Teil des Unionsrechts.“⁹⁸⁶

Das Grundrecht auf Datenschutz wird aus dem „Anspruch auf Achtung des Privat- und Familienlebens“ hergeleitet. Der Schutzzweck des § 1 Abs 1 DSG geht aber deutlich über jenen des Art 8 EMRK hinaus, da zusätzlich zum Bereich des Privat- und Familienlebens auch der Bereich des wirtschaftlichen und politischen Lebens eingeschlossen sind.⁹⁸⁷

Fand sich in § 1 Abs 1 DSG idF DSG 1978 lediglich am Satzende der Verweis „(...) schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens (...)“, ist dieser Bereich in der aktuellen Fassung deutlich erweitert und an den Satzanfang gestellt: „(...) insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht (...)“.⁹⁸⁸

Die praktische Bedeutung der Abgrenzung der Schutzbereiche des § 1 DSG und des Art 8 EMRK besteht nicht, da die in § 1 Abs 2 DSG normierten Regeln zur Rechtfertigung staatlicher Eingriffe in das Grundrecht auf Datenschutz auf die Rechtfertigungsanforderungen des Art 8 Abs 2 EMRK verweisen und teilweise über sie hinausgehen.⁹⁸⁹

⁹⁸⁵ Vgl BGBl Nr 59/1964.

⁹⁸⁶ Art 6 Abs 3 EUV.

⁹⁸⁷ Vgl *Wiederin*, Schutz der Privatsphäre, in: *Merten/Papier*, HGR VII/1, § 190 Rz 136 mwN.

⁹⁸⁸ *Wiederin*, Schutz der Privatsphäre, in: *Merten/Papier*, HGR VII/1, § 190 Rz 136 mwN.

⁹⁸⁹ *Wiederin*, Schutz der Privatsphäre, in: *Merten/Papier*, HGR VII/1, § 190 Rz 139 mwN.

3. Charta der Grundrechte der Europäischen Union

In Artikel 6 Abs 1 EUV findet sich nach dem Vertrag von Lissabon⁹⁹⁰ ein Verweis auf die Charta der Grundrechte.⁹⁹¹ Darin heißt es, dass die Union die Rechte, Freiheiten und Grundsätze anerkennt, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind. Die Verträge der Europäischen Union und die Charta der Grundrechte sind rechtlich gleichrangig, wobei die in den Verträgen festgelegten Zuständigkeiten der Union in keiner Weise erweitert werden.⁹⁹² Zur Auslegung der in der Charta niedergelegten Rechte, Freiheiten und Grundsätze verweist Art 6 EUV auf die allgemeinen Bestimmungen des Titels VII der Charta und auf die in der Charta angeführten Erläuterungen, in denen die Quellen dieser Bestimmungen angegeben sind.

Auch wurde durch Art 6 Abs 2 EUV die Europäische Union verpflichtet,⁹⁹³ als Ganzes der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten beizutreten, wobei dieser Beitritt nicht die in den Verträgen festgelegten Zuständigkeiten der Union ändert.⁹⁹⁴

Zwischen Juli 2010 und Juni 2011 führte eine informelle Arbeitsgruppe insgesamt acht Treffen mit der Europäischen Kommission durch.⁹⁹⁵ Schließlich leitete das Ministerkomitee das Komitee für Menschenrechte (CDDH) an, die Verhandlungen mit der Europäischen Union in einer ad hoc Gruppe „47+1“ fortzuführen.⁹⁹⁶ Ein erstes Verhandlungstreffen zwischen CDDH und der Europäischen Kommission wurde am 21. Juni 2012 abgehalten, um sich auf den Ablauf der künftigen Treffen und andere prozessualer Angelegenheiten zu klären.⁹⁹⁷ Laufende Arbeitsdokumente können online eingesehen werden.⁹⁹⁸

⁹⁹⁰ Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13. Dezember 2007 (= ABI C 306 vom 17.12.2007, S 1-271).

⁹⁹¹ Vgl auch V.E Reform des „europäischen Datenschutzrechtes“.

⁹⁹² Vgl Art 6 Abs 1 Satz 1 und 2 EUV.

⁹⁹³ Art 6 Abs 2 EUV postuliert: „Die EU tritt der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten bei.“

⁹⁹⁴ Art 6 Abs 2 EUV.

⁹⁹⁵ http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/default_en.asp - „The negociation process“ (Stand: 18.08.2013).

⁹⁹⁶ http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/default_en.asp - „The negociation process“ (Stand: 18.08.2013).

⁹⁹⁷ http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/default_en.asp - „The negociation process“ (Stand: 18.08.2013).

⁹⁹⁸ http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/Working_documents_en.asp (Stand: 18.08.2013).

Noch ist die Europäische Union nicht beigetreten,⁹⁹⁹ wemngleich Art 6 Abs 3 EUV die Verbindlichkeit der Europäischen Menschenrechtskonvention schon nach derzeitigem Stand vorschreibt. So erwähnt Art 6 Abs 3 EUV, dass „die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben,“¹⁰⁰⁰ als allgemeine Grundsätze Teil des Unionsrechts sind. Auch das Stockholmer Programm erachtet es als wichtig, dass die Union möglichst rasch der EMRK beitrifft, wodurch die Verpflichtung der Union, einschließlich der Organe, sichergestellt werden soll, dass in sämtlichen Tätigkeitsbereichen die Grundrechte und Grundfreiheiten aktiv vorangebracht werden.¹⁰⁰¹

Die für den Bereich des Datenschutzes besonders relevanten Bestimmungen der Charta der Grundrechte der Europäischen Union sind folgende Artikel:

Artikel 7¹⁰⁰² der Grundrechte-Charta (GRCh) trägt den Titel „Achtung des Privat- und Familienlebens“ und lautet:

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8¹⁰⁰³ GRCh trägt den Titel „Schutz personenbezogener Daten“ und lautet:

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

⁹⁹⁹ Vgl. <http://conventions.coe.int/Treaty/Commun/ListeTableauCourt.asp?MA=3&CM=16&CL=ENG> (Stand: 18.08.2013).

¹⁰⁰⁰ Art 6 Abs 3 EUV.

¹⁰⁰¹ Souhrada-Kirchmayer in ÖJK (Hg), Grundrechte im Europa der Zukunft, 129 (130).

¹⁰⁰² Konsolidierte Fassung der Charta der Grundrechte der Europäischen Union, Artikel 7 – Achtung des Privat- und Familienlebens (= ABl C 83 vom 30.03.2010, S 393).

¹⁰⁰³ Konsolidierte Fassung der Charta der Grundrechte der Europäischen Union, Artikel 8 - Schutz personenbezogener Daten (= ABl C 83 vom 30.03.2010, S 393).

Ähnlich der Abgrenzung zwischen § 1 DSG und Art 8 EMRK schützt Art 7 GRCh nur den Bereich des Privat- und Familienlebens, der Wohnung sowie der Kommunikation (in Art 8 EMRK: „Briefverkehr“). Der Schutz auch anderer Bereiche umfassender Daten wird in Art 8 GRCh statuiert, weshalb dieser einen weiteren Anwendungsbereich umfasst.

Besonders zu erwähnen ist die jüngste Rsp des österr VfGH: Im Unterschied zur bisherigen Rechtsansicht, wonach Unionsrecht keinen Maßstab seiner Rechtskontrolle bildete, geht der VfGH nun davon aus, dass die am 1.12.2009 in Kraft getretene GRCh Rechte garantiere, die vor dem VfGH als verfassungsgesetzlich gewährleistete Rechte geltend gemacht werden können.¹⁰⁰⁴ Der VfGH betont, dass die GRCh „innerhalb des Unionsrechts einen von den <Verträgen> deutlich abgegrenzten Bereich“¹⁰⁰⁵ bildet.

Aufgrund der unterschiedlichen Struktur der in der GRCh verbürgten Rechte (Art 22 und Art 37 GRC nennen etwa nur Grundsätze zur Vielfalt der Kulturen, Religionen und Sprachen sowie zum Umweltschutz) prüft der VfGH jeweils im Einzelfall, ob österreichische Vorschriften aufzuheben sind, da sie gegen bestimmte in der GRCh garantierte Rechte verstoßen.¹⁰⁰⁶

Die vom VfGH erfolgte Argumentation, dass die GRCh und die Verträge einen deutlich abgegrenzten Bereich darstellen, übersieht Wesentliches. So wird als Argument angeführt, dass Art 6 Abs 1 EUV „die Charta der Grundrechte und die Verträge“ nenne. Hierbei wird jedoch nicht beachtet, dass sich diese Aufzählung in Art 6 Abs 1 EUV mit „sind rechtlich gleichrangig“ fortsetzt. Eine unterschiedliche rechtliche Bedeutung ist daher mE von den Urhebern der Bestimmung gerade nicht gewollt.

Im Ergebnis schließe ich mich jedoch dem VfGH an, da durch die Möglichkeit der Berufung auf die GRCh der Inhalt der österr Grundrechte erhellt und auch aktualisiert werden kann. Aus rechtspolitischer Sicht stellt die neue Rsp des VfGH einen wesentlichen Fortschritt für die Achtung der Grundrechte dar, da die GRCh einen „modernen und umfassenden Grundrechtskatalog“¹⁰⁰⁷ enthält, der auch aktuelle Gefährdungslagen berücksichtigt.¹⁰⁰⁸ Schwierig bleibt allerdings die Bemerkung des VfGH, wonach im Anlassfall zu entscheiden ist, welche Rechte der GRCh einen Prüfungsmaßstab für das Verfahren vor dem VfGH bilden können. Somit kann der Rechtsanwender sich erst dann auf ein in der GRCh verbürgtes Recht

¹⁰⁰⁴ *Lehofer*, VfGH: EU-Grundrechte-Charta als Prüfungsmaßstab, ÖJZ 2012, 433 (433).

¹⁰⁰⁵ VfGH 14.03.2012, U 466/11ua, 5. Punkt.

¹⁰⁰⁶ *Lehofer*, VfGH: EU-Grundrechte-Charta als Prüfungsmaßstab, ÖJZ 2012, 433 (433).

¹⁰⁰⁷ *Wolffgang* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Anh zu Art 6 EUV Rz 10.

¹⁰⁰⁸ Vgl *Wolffgang* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Anh zu Art 6 EUV Rz 10.

stützen, wenn es sich dabei nicht um einen bloßen „Grundsatz“ handelt, sondern (jedenfalls) dann, „wenn die betreffende Garantie der Grundrechte-Charta in ihrer Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleicht“¹⁰⁰⁹ ¹⁰¹⁰.

Dass in Art 8 GRCh ausdrücklich auch das Recht auf informationelle Selbstbestimmung normiert wird, spiegelt die grundrechtliche Bedeutung dieser Thematik wider. Art 8 GRCh unterscheidet sich somit vom Grundrecht auf Achtung des Privat- und Familienlebens (vgl Art 7 GRCh) und normiert ein eigenständiges „Grundrecht jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten.“¹⁰¹¹ Durch Art 6 EUV wird auch Art 8 GRCh rechtlich verbindlich, wodurch die EU zur Gewährleistung eines in allen Bereichen gleichwertigen Schutzes des Grundrechts auf Datenschutz verpflichtet wurde.¹⁰¹² Die Rechtsgrundlage für Datenschutzrechtsakte auf hohem und vereinheitlichtem Schutzniveau innerhalb der EU stellt Art 16 AEUV dar,¹⁰¹³ dessen Abs 1 wörtlich mit Art 8 Abs 1 GRCh übereinstimmt.¹⁰¹⁴

Art 8 Abs 2 GRCh regelt Schranken der Grundrechtseingriffe und normiert gewisse Rechte des Betroffenen gegenüber dem Datenverwender.¹⁰¹⁵ Abs 3 *leg cit* verpflichtet die Union und die Mitgliedstaaten zur Einrichtung einer unabhängigen Stelle, die die Einhaltung dieser Vorschriften überwacht.¹⁰¹⁶

Zum Verhältnis von Art 8 GRCh zu Art 8 EMRK ist anzumerken, dass Art 8 GRCh für den Bereich der datenschutzrechtlichen Aspekte im Privatleben auf den bestehenden Schutzgarantien des Art 8 Abs 1 EMRK aufbaut, und ihn um weitere datenschutzrechtliche Aspekte ergänzt, wohingegen andere Konventionsgarantien des Art 8 Abs 1 EMRK in Art 7 GRCh normiert wurden.¹⁰¹⁷

¹⁰⁰⁹ VfGH 14.03.2012, U 466/11ua, 5.5. Punkt sowie *Lehofer*, VfGH: EU-Grundrechte-Charta als Prüfungsmaßstab, ÖJZ 2012, 433 (433).

¹⁰¹⁰ Vgl bereits *B. Raschauer* in *ÖJK (Hg)*, Grundrechte im Europa der Zukunft, 59 (62 ff).

¹⁰¹¹ *Zerdick* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Art 16 AEUV Rz 2.

¹⁰¹² Vgl auch *Zerdick* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Art 16 AEUV Rz 6.

¹⁰¹³ Vgl auch *Zerdick* in *Lenz/Borchardt (Hrsg)*, EU-Verträge⁵ Art 16 AEUV Rz 6 f.

¹⁰¹⁴ Vgl auch V.E Reform des „europäischen Datenschutzrechtes“.

¹⁰¹⁵ Vgl *Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern - heute - morgen, 381 (384).

¹⁰¹⁶ *Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern - heute - morgen, 381 (384).

¹⁰¹⁷ Ebenso: *Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern - heute - morgen, 381 (387 f).

Bei der Interpretation von Art 8 GRCh sind insbesondere die Datenschutzrichtlinie¹⁰¹⁸ und die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr¹⁰¹⁹ zu beachten, die auf Basis des damaligen Art 286 Abs 2 EGV erlassene datenschutzrechtsspezifische Sekundärrechtsakte darstellen.¹⁰²⁰

Zu betonen ist, dass Art 8 GRCh im Unterschied zur RL 1995/46/EG „jeder Person“ das Recht auf Schutz der sie betreffenden personenbezogenen Daten einräumt. Die RL 1995/46/EG schützt jedoch nur Daten natürlicher Personen. Im Anschluss an *B. Raschauer* und *N. Raschauer* könnte die Datenschutz-RL künftig chartakonform zu interpretieren sein und somit auch personenbezogene Daten juristischer Personen einbeziehen.¹⁰²¹

Die Charta ist aber im Einklang mit dem historisch gewachsenen Primär- und dem daraus abgeleiteten Sekundärrecht zu sehen. Diese zum Zeitpunkt des Inkrafttretens der Charta bereits bestandenen Regelungen sind bei der Interpretation der Bestimmungen der Charta zu berücksichtigen, weshalb davon auszugehen ist, dass die Charta den Anwendungsbereich der Datenschutz-RL nicht auf juristische Personen erweitern wollte¹⁰²² und somit personenbezogene Daten juristischer Personen nur insoweit geschützt werden, als dies zum Zeitpunkt des Inkrafttretens der Charta bereits geltendes Gemeinschafts- bzw Unionsrecht war.¹⁰²³

¹⁰¹⁸ 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 (= ABI L 281 vom 23.11.1995, S 31-50).

¹⁰¹⁹ Verordnung (EG) Nr 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (= ABI L 8 vom 12.1.2001, S 1-22).

¹⁰²⁰ Zu weiteren für die Interpretation bedeutsamen Rechtsakten und Rechtsakten mit „interpretationsleitender Funktion“ sowie konkreten Beispielen: *Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern – heute – morgen, 381 (385 ff sowie 392 f).

¹⁰²¹ *B. Raschauer* in *ÖJK (Hg)*, Grundrechte im Europa der Zukunft, 59 (62) mit Verweis auf *N. Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern - heute - morgen, 381 (389).

¹⁰²² Ebenso: *B. Raschauer* in *ÖJK (Hg)*, Grundrechte im Europa der Zukunft, 59 (64).

¹⁰²³ Weitere hierfür sprechende Argumente finden sich bei *N. Raschauer* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern - heute - morgen, 381 (389 f).

B. Datenschutz und Technik

Bevor ich nun die wesentlichen Thesen meiner Arbeit nochmals hervorhebe, werde ich auf technische Aspekte im Zusammenhang mit dem verfassungsgesetzlich gewährleisteten Datenschutzrecht eingehen.

Die grundrechtliche Sicherung der Datenschutzrechte hängt eng mit der technischen Sicherheit der verwendeten Systeme zusammen. Verantwortliche Organwalter von Unternehmen haben jedenfalls dafür zu sorgen, dass eine dem Stand der Technik entsprechende IT besteht, um die ständige Verfügbarkeit, die Vertraulichkeit sowie die Unversehrtheit der Daten zu gewährleisten, wobei Unterlassungen zur Haftung für den dadurch verursachten Schaden führen,¹⁰²⁴ was auch in der Schweiz so vertreten wird.¹⁰²⁵ Besonders bei Kooperationen ist aus haftungsrechtlicher Sicht im Zusammenhang mit dem jeweils aktuellen Stand der Technik Vorsicht geboten.¹⁰²⁶ (Daten-)Sicherheit ist somit kein Zustand, sondern ein Prozess.¹⁰²⁷

Zu vergessen ist aber auch nicht der körperliche Diebstahl von Hardware, um sich Zugang zu gespeicherten Daten zu verschaffen – besondere Sicherheitsmaßnahmen sind zur Vermeidung von unbefugtem Zugang oder Zugriff erforderlich.¹⁰²⁸

„Datenschutz ist eine Grundbedingung für die Freiheitsausübung in einer demokratischen Gesellschaftsordnung und damit für die Existenz dieser Gesellschaftsordnung selbst.“¹⁰²⁹

¹⁰²⁴ Vgl *Hasberger*, IT-Sicherheit und Haftung, *ecolex* 2007, 508 (510).

¹⁰²⁵ *Holliger-Hagmann*, Bankenhaftung: Vorsicht mit den Kundendaten, *Schweizer Bank* 07/2006, 42 (42 f).

¹⁰²⁶ *Holliger-Hagmann*, Bankenhaftung: Vorsicht mit den Kundendaten, *Schweizer Bank* 07/2006, 42 (43).

¹⁰²⁷ *Hansen/Neumann*, *Wirtschaftsinformatik* 1¹⁰, 384.

¹⁰²⁸ Vgl *Hansen/Neumann*, *Wirtschaftsinformatik* 1¹⁰, 405.

¹⁰²⁹ *Hansen/Neumann*, *Wirtschaftsinformatik* 1¹⁰, 418.

VII. Schlussfolgerungen

Einige der in meiner Arbeit angesprochenen Schlussfolgerungen werde ich abschließend nochmals hervorheben und dabei die aktuellen Probleme sowie konkrete Verbesserungsmöglichkeiten aufzeigen:

A) Informationsverbundsysteme:

1) ME sind gesetzliche Regelungen für die Zulässigkeit von Bonitätsdatenbanken erforderlich. Neben den von *Kotschy*¹⁰³⁰ angesprochenen Regelungsbereichen sehe ich als Unterpunkt zur Frage, welche Daten verarbeitet werden dürfen, auch Bagatellgrenzen für die Zulässigkeit von Negativdaten als sinnvoll an. Für Positivdaten ist auf die laut Genehmigungsbescheid der DSK für die Kleinkreditevidenz bestehende Auflage, wonach erst Kreditverträge oder abgelehnte Kreditanträge ab EUR 300,00 eingetragen werden können, zu verweisen. Negativeinträge haben eine sehr hohe Eingriffsintensität und sind daher bei nicht fristgerecht erfolgten Zahlungen jedenfalls im Ausmaß von bis zu EUR 100,00 nicht verhältnismäßig.

2) In Deutschland besteht der kurzfristige Zahlungsausgleich, wonach eine frühzeitige Löschung eines nur kurzfristig (bis maximal sechs Wochen) bestehenden Zahlungsanstandes bis EUR 1.000,00 erfolgt. Eine ähnliche Regelung sollte in Österreich geschaffen werden.

B) Zum Datenschutzgesetz und dem „automatischen Datenaustausch im Bereich der Finanzdienstleistungen“:

1) Nach grundlegender Auseinandersetzung mit den datenschutzrechtlichen Bestimmungen sehe ich es nach wie vor als sehr komplexe Materie an. Dazu tragen mE auch unterschiedliche nationale und europäische Terminologien bei. Ich spreche mich daher zur leichteren Verständlichkeit für die Rechtsanwender für die Verwendung einheitlicher Terminologien aus. Markantestes Beispiel ist etwa die inhaltliche Übereinstimmung der Wörter „Verwenden“ (österr DSG) und „Verarbeiten“ (RL). Inwiefern die österr Kreation von „Verwenden“ als Überbegriff sinnvoll war, kann von mir nicht nachvollzogen werden. Die europäische Datenschutzverordnung kann – sofern sie beschlossen werden wird – dadurch,

¹⁰³⁰ *Kotschy*, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 307 (310 ff).

dass sie einheitliche Regelungen vorgibt und nicht national umgesetzt werden muss, solche Unklarheiten beseitigen und vermeiden.

2) Nach § 8 Abs 1 Z 4 DSG werden schutzwürdige Geheimhaltungsinteressen nicht verletzt, wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. Gemäß Art 7 lit f der RL 1995/46/EG kann, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten des Betroffenen überwiegen, eine Verarbeitung zur Verwirklichung eines berechtigten Interesses des Auftraggebers oder Dritten durchgeführt werden. Somit ist nach der RL eine Datenverarbeitung auch dann zulässig, wenn die Interessen des Auftraggebers oder eines Dritten gleich wiegen, wie jene des Betroffenen. Ich spreche mich daher für eine entsprechende Anpassung des österr DSG aus, damit künftig die Verwendung von Daten solange zulässig ist, als die Interessen des Betroffenen nicht überwiegen oder eine Änderung der RL, um Rechtskonformität zu wahren.

3) Die taxative Aufzählung in § 8 Abs 3 DSG würde ich der Vollständigkeit halber auch auf vorvertragliche Maßnahmen, die vom Betroffenen ausgehen, erweitern. Hierzu ist eine Ergänzung von § 8 Abs 3 Z 4 DSG zu bevorzugen, der derzeit schutzwürdige Geheimhaltungsinteressen insbesondere dann nicht verletzt sieht, wenn die Verwendung von Daten zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist. Die sekundärrechtliche Grundlage bietet Art 7 lit b der RL 1995/46/EG, der die Verarbeitung personenbezogener Daten auch für den Fall der Durchführung vorvertraglicher Maßnahmen, die auf Antrag des Betroffenen erfolgen, erlaubt.

4) Die Richtlinienkonformität von § 28 Abs 2 DSG ist aus den in meiner Arbeit dargelegten Gründen¹⁰³¹ zu bezweifeln. Die in Art 14 lit a der RL 1995/46/EG eingeräumte Möglichkeit einer „im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung“ ermöglicht mE kein Widerspruchsrecht im Umfang des § 28 Abs 2 DSG. § 28 Abs 2 DSG muss daher, sofern es sich nicht um Zwecke der Direktwerbung handelt (vgl Art 14 lit b der RL 1995/46/EG), verfassungskonform mittels § 1 Abs 2 DSG interpretiert werden, der bei Eingriffen in das Grundrecht eine Interessenabwägung vorsieht.

5) Soweit personenbezogene Daten durch das Inland nur durchgeführt werden, ist das DSG nicht anwendbar (§ 3 Abs 3 DSG). Eine Konkretisierung dieser Bestimmung wäre

¹⁰³¹ Vgl IV.E.4 Judikatur der österr DSK.

wünschenswert, damit zur Interpretation nicht der Begriff der „reinen Durchleitung“ in Art 12 der E-Commerce-Richtlinie 2000/31/EG herangezogen werden muss.

6) Die Anpassung der österr DSAV war längst notwendig und wurde erst durch die DSAV-Novelle 2013 an die zahlreichen Entscheidungen der Europäischen Kommission angepasst. Durch die Entscheidungen wurde festgestellt, welche Staaten über ein angemessenes Datenschutzniveau verfügen. Dies erleichtert (leider erst seit 2013) den Umgang für den Rechtsanwender iZm Datenübermittlungen in Drittstaaten und hat zur Klarheit wesentlich beitragen.

7) Bei der Verwendung von Standardvertragsklauseln sieht die österr DSK eine Genehmigungspflicht vor. Zur Beschleunigung des Verfahrens ist bei wortgleicher Übernahme der Standardvertragsklauseln eine Anzeigepflicht der bisherigen Genehmigungspflicht vorzuziehen.

8) Die Unabhängigkeit der österr DSK wurde durch Urteil des EuGH in einem Verfahren der Europäischen Kommission gegen die Republik Österreich wegen mangelnder Umsetzung der in der RL 1995/46/EG vorgesehenen völligen Unabhängigkeit der Kontrollstellen (Art 28 Abs 1 der RL 1995/46/EG) festgestellt. Die Verwaltungsgerichtsbarkeits-Novelle 2012 sowie die DSG-Novellen bringen wichtige Änderungen mit sich. Insbesondere die Bedenken der Europäischen Kommission zum Unterrichtsrecht des Bundeskanzlers sind mE nach wie vor ernst zu nehmen.

9) Zur Quellensteuer: Die Quellensteuer wird trotz der im Vergleich zur österr KEST iHv 25 % relativ hohen Besteuerung von 35 % auf Zinserträge noch längere Zeit Bestandteil des österr Rechts sein, da sie nach wie vor Steuervorteile mit sich bringt. Aus Sicht der Steuergerechtigkeit wäre die automatische Auskunftserteilung sinnvoller. Dadurch könnte eine Besteuerung erreicht werden, die der tatsächlichen Steuerpflicht entspricht, wodurch eine Besteuerung der Zinserträge mit dem Spitzensteuersatz von rund 50 % möglich wäre. Datenschutzrechtliche Bedenken und solche iZm dem Bankgeheimnis können mE durch folgende Maßnahmen ausgeräumt werden: Die Gegenstand der Auskunft bildenden Daten sind genau in Art 8 der RL 2003/48/EG geregelt; hierbei sind hohe technische Sicherheitsstandards einzuhalten. Auch wird die Auskunft lediglich an die zuständigen Finanzbehörden der EU-Mitgliedstaaten erteilt.

C) *Regelungen im internationalen Kontext:*

1) Die Datenschutz-VO kann unterschiedliche nationale Umsetzungen von RL-Bestimmungen lösen, wenngleich insgesamt eine Annäherung auf dem kleinsten gemeinsamen Konsens aller EU-Mitgliedstaaten zu befürchten ist, was eine Absenkung des österr Datenschutzniveaus zur Folge hätte. Es ist daher genau auf die Regelungsbereiche der Datenschutz-VO zu achten.

2) Abkommen mit der Schweiz:

Die politische Ablehnung Österreichs iZm der Einführung des automatischen Informationsaustausches führt zu anderen Wegen, um im Ausland bestehende Vermögen und vor allem Zinseinkünfte von in Österreich wohnhaften natürlichen Personen zu besteuern. Unter den gegebenen Voraussetzungen ist das Abkommen mit der Schweiz sinnvoll. Meiner Meinung nach ist jedoch längerfristig ein automatischer Informationsaustausch durchzuführen, was eine direkte Zuordnung zur steuerpflichtigen Person ermöglicht. Der derzeitige politische Konsens hat den automatischen Informationsaustausch zwischen Österreich und der Schweiz in weitere Entfernung gerückt. Politische Zugeständnisse Luxemburgs und Österreichs müssten gemacht werden.

3) SWIFT

a) Um eine von Europol erteilte Bestätigung, welche SWIFT dazu verpflichtet, dem US-Finanzministerium gewisse Daten bereitzustellen, im Nachhinein überprüfen zu können, müssen nachvollziehbare schriftliche Aufzeichnungen über die Ersuchen geführt werden, die eine nachträgliche Beurteilung der Entscheidungsfindung ermöglichen. Die Aufzeichnungen müssen die Gründe für die Zulässigkeit gem Art 4 Abs 2 des SWIFT-Abkommens 2010 belegen.

b) Der hohe Geheimhaltungsgrad erschwert die Offenlegung gegenüber Dritten und somit auch gegenüber der Öffentlichkeit. Dies muss durch weitgehende Kontrollbefugnisse des Europäischen Datenschutzbeauftragten und der Gemeinsamen Kontrollinstanz von Europol ausgeglichen werden.

c) Die bestehenden Auskunftsrechte nach dem SWIFT-Abkommen ermöglichen durch die Einschränkung der „angemessenen rechtlichen Beschränkungen“ de facto kein Auskunftsrecht der Betroffenen, wodurch eine effektive Strafverfolgung ermöglicht werden soll. Dies müsste durch weiterreichende nachträgliche Auskunftspflichten gegenüber den Betroffenen ausgeglichen werden.

Literaturverzeichnis

- Aigner, Dietmar J.*, Europäische Kommission schlägt Änderungen der Sparzinsenrichtlinie zur Verhinderung der Steuerflucht vor, SWI 2008, 571.
- Aigner, Dietmar J.*, Habilitationsschrift: Die SparzinsenRL – Koordinierung der Besteuerung von Zinsen in Europa, taxlex 2009, 540.
- Aigner, Dietmar J.*, Kommission veröffentlicht Bericht zur Überprüfung der Sparzinsenrichtlinie, SWI 2008, 505.
- Aigner, Dietmar J.*, Problembereiche bei der Behandlung von Trusts und Stiftungen im Anwendungsbereich der Sparzinsenrichtlinie, ZfS 2009, 59.
- Andréewitch, Markus / Steiner, Gerald*, Internationaler Datentransfer: Neue „alternative“ Standardvertragsklauseln, RdW 2006, 81.
- Apathy, Peter*, Abtretung von Bankforderungen und Bankgeheimnis, ÖBA 2006, 33.
- Apathy, Peter*, Auswirkungen der Judikatur zu Verbraucherverträgen auf Bankgeschäfte mit Unternehmern, ÖBA 2004, 737.
- Apathy, Peter*, Die neuen ABB auf dem Prüfstand – Anmerkungen zu OGH 4 Ob 179/02f, ÖBA 2003, 177.
- Appl, Clemens*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 96.
- Bachmann, Susanne / Baumgartner, Gerhard / Feik, Rudolf / Giese, Karim J. / Jahnel, Dietmar / Lienbacher, Georg (Herausgeber)*, Besonderes Verwaltungsrecht, 8., aktualisierte Auflage, Verlag Springer, Salzburg/Wien 2010; zitiert: *Autor* in *Bachmann et altera*, Besonderes Verwaltungsrecht⁸ (2010), [Seite].
- Bachner, Thomas*, Aktienrechts-Änderungsgesetz beschlossen! – Die wichtigsten Neuerungen, GeS 2009, 248.
- Bammer, Armin / Holzinger, Gerhart / Vogl, Mathias / Wenda, Gregor*, Rechtsschutz gestern – heute – morgen: Festgabe zum 80. Geburtstag von Rudolf Machacek und Franz Matscher, NWV Neuer Wissenschaftlicher Verlag, Wien / Graz 2008; zitiert: *Autor* in *Bammer/Holzinger/Vogl/Wenda (Hg)*, Rechtsschutz gestern – heute – morgen, [Seite].
- Barbist, Johannes*, EuGH zur Vorratsdatenspeicherung – Das Urteil in der Rechtssache Irland gegen Europäisches Parlament/Rat der Europäischen Union, MR 2009, 3.

- Bauer, Lukas / Reimer, Sebastian (Herausgeber)*, Handbuch Datenschutzrecht, facultas.wuv Universitätsverlag, Wien 2009; zitiert: *Autor* in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009) [Seite].
- Beiser, Reinhold*, Schafft eine Zusammenarbeit zwischen Österreich und der Schweiz mehr Gleichheit?, RdW 2012, 361.
- Bergmann, Sebastian*, Steuerhinterziehungs- und Missbrauchsterminologie im europäischen Steuerrecht, SWI 2010, 477.
- Berka, Walter / Höhne, Thomas / Noll, Alfred J. / Polley, Ulrich*, Mediengesetz – Praxiskommentar, 2., aktualisierte Auflage, Verlag LexisNexis ARD Orac, Wien 2005; zitiert: *Berka/Höhne/Noll/Polley*, Mediengesetz² [§], [Rz], [Seite].
- Birnbauer, Wilhelm*, Das Aktienrechts-Änderungsgesetz 2009 (AktRÄG 2009) – Auszüge im Überblick, ÖRPfl 2010 H 2, 33.
- Bollenberger, Raimund / Kellner, Markus*, OGH 19.05.2010, 6 Ob 2/10b, ÖBA 2010, 853.
- Brandl, Ernst / Knoll, Martin*, Datenschutzrechtliche Grenzen der FMA-Prüfung, ecolex 2009, 443.
- Brenn, Christoph*, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ 1997, 641.
- Brodil, Wolfgang*, Datenschutzrechtliche Aspekte der Verwendung von Gesundheitsdaten im Arbeitsverhältnis, ecolex 2010, 122.
- Büllesbach, Alfred (Herausgeber)*, Datenverkehr ohne Datenschutz? – Eine globale Herausforderung, Verlag Dr. Otto Schmidt, Köln/Stuttgart 1999; in: Informationstechnik und Recht, Schriftenreihe der Deutschen Gesellschaft für Recht und Informatik e. V., Band 8; zitiert: *Autor* in *Büllesbach (Hrsg)*, Datenverkehr ohne Datenschutz?, [Seite].
- Derleder, Peter / Knops, Kai-Oliver / Bamberger, Heinz Georg (Herausgeber)*, Handbuch zum deutschen und europäischen Bankrecht, 2. Auflage, Verlag Springer, Berlin / Heidelberg 2009; zitiert: *Autor* in *Derleder/Knops/Bamberger (Hg)*, Handbuch Bankrecht, [§], [Rz], [Seite].
- Dohr, Walter / Pollirer, Hans-Jürgen / Weiss, Ernst M. / Knyrim, Rainer*, Datenschutzrecht: Kommentar, 2., völlig neu bearbeitete Auflage mit 12. Ergänzungslieferung (Dezember 2011), Datenschutzgesetz 2000 samt Europarecht, Nebengesetzen, Verordnungen und Landesdatenschutz; mit Prüflisten und Mustern für die Praxis ergänzt; auf Grundlage der Manzschen Sonderausgabe Datenschutzgesetz (1988),

- Verlag Manz (Loseblattausgabe), Wien 2002; zitiert: *Dohr/Pollirer/Weiss/Knyrim*, DSG² [§], [Anm, E bzw Anh], [Seite].
- Drobesch, Heinz / Grosinger, Walter*, Das neue österreichische Datenschutzgesetz: Datenschutzgesetz 2000, Datenverarbeitungsregister-Verordnung, Datenschutzangemessenheits-Verordnung, Standard- und Muster-Verordnung, EG-Datenschutzrichtlinie uvm; mit ausführlichem Kommentar und Erläuterungen in übersichtlicher Gliederung und großem Stichwortverzeichnis, Verlag Juridica, Wien 2000; zitiert: *Drobesch/Grosinger*, Datenschutzgesetz [§], [Seite].
- Duschanek, Alfred / Rosenmayr-Klemenz, Claudia*, Datenschutzgesetz 2000 – DSG 2000: Bundesgesetz über den Schutz personenbezogener Daten, Gesetzestext samt Einführung und Kurzkomentar, in: Wissenschaftliche Reihe: Wissenschaft und Wirtschaftspraxis, Wirtschaftskammer Österreich, Band 6, zitiert: *Duschanek/Rosenmayr-Klemenz*, DSG 2000, [Seite].
- Duschanek, Alfred*, § 1 DSG 2000, in: *Korinek, Karl / Holoubek, Michael (Hrsg)*, Österreichisches Bundesverfassungsrecht: Textsammlung und Kommentar, Verlag Springer, Wien 1999 (Loseblattausgabe – 5. Lieferung 2007); zitiert: *Duschanek*, § 1 DSG 2000 [Rz], [Seite].
- Eilmansberger, Thomas et altera, Studiengesellschaft für Wirtschaft und Recht (Herausgeber)*, Geheimnisschutz, Datenschutz, Informationsschutz, Verlag Linde, Wien 2008; zitiert: *Autor in Eilmansberger et altera*, Geheimnisschutz, Datenschutz, Informationsschutz, [Seite].
- Ellger, Reinhard*, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem Europäischen Datenschutzrecht, *RabelsZ* 1996, 738.
- Ennöckl, Daniel*, EuGH zur Veröffentlichung von EU-Agrarbeihilfen: (vorläufiges) Ende der Transparenz, *ÖJZ* 2011, 955.
- Fragner, Julia / Schimka, Matthias*, Finanzausschuss beschließt Initiativantrag zum Amtshilfe-Durchführungsgesetz, *GesRZ* 2009, 195.
- Frey, Eric*, Schweiz schaltet beim Bankgeheimnis jetzt auf hart. Steuerexperte sieht viel Widerstand gegen automatischen Informationsaustausch – Anfragen müssen spezifisch sein, *DerStandard* 2009/43/01.
- Friedl, Gerhard / Loebenstein, Herbert (Hrsg.)*, Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen (AZR), 7. Auflage, Verlag Manz, Wien 2012; zitiert: *Friedl/Loebenstein*, Abkürzungs- und

- Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen (AZR)⁷ (2012).
- Funke, Andreas*, Umsetzungsrecht: Zum Verhältnis von internationaler Sekundärrechtsetzung und deutscher Gesetzgebungsgewalt, Mohr Siebeck, Tübingen 2010; zitiert: *Funke*, Umsetzungsrecht, [Seite].
- Gläser, Lars*, EU-Zinsenbesteuerung – Vermeidung der Doppelbesteuerung, SWI 2005, 325.
- Gläser, Lars*, Handbuch der EU-Quellensteuer: Leitfaden für Wissenschaft und Praxis, Verlag Linde, Wien 2006; zitiert: *Gläser*, Handbuch der EU-Quellensteuer, [Seite].
- Grabovickic, Boris / Dugonjic, Mirsada / Zinnöcker, Lisa*, Bankenaufsicht in Österreich – Berichte und Analysen, ÖBA 2009, 425.
- Graf, Georg*, Jetzt schlägt's aber (fast) 13! – Geschäftsbedingungen der Kreditinstitute: OGH erklärt 12 Klauseln der Banken AGB 2000 für unwirksam, ecolex-Script 2003/24; zitiert: *Graf*, Jetzt schlägt's aber (fast) 13!, ecolex-Script 2003/24, [Seite].
- Graf, Wolfgang*, Datenschutzrecht im Überblick, 2., überarbeitete Auflage, facultas.wuv Universitätsverlag, Wien 2010; zitiert: *Graf*, Datenschutzrecht im Überblick² (2010) [Seite].
- Gruber, Philip / Vondrak, Philip*, Initiativantrag zum Amtshilfe-Durchführungsgesetz eingebracht, SWK 2009, T 153.
- Hackl, Günther*, Der „gläserne Unternehmer“, SWK 2009, T 63.
- Hänni, Urs P. / Jans, Victor*, Wie sicher ist das Internet? Die Auswirkungen der Vernetzung auf die Informatik-Sicherheit, VWT 1996 Heft 4, 21.
- Hansen, Hans Robert / Neumann, Gustaf*, Wirtschaftsinformatik 1 – Grundlagen und Anwendungen, 10., völlig neu bearbeitete und erweiterte Auflage, Lucius & Lucius UTB Verlag, Wien 2009; zitiert: *Hansen/Neumann*, Wirtschaftsinformatik 1¹⁰, [Seite].
- Hasberger, Michael*, IT-Sicherheit und Haftung, ecolex 2007, 508.
- Hassemer, Winfried*, Strafrecht im Wandel, JRP 2007, 79.
- Heidenbauer, Sabine*, Internationale Aspekte der EU-Quellensteuer, SWI 2006, 459.
- Heissl, Gregor (Herausgeber)*, Handbuch Menschenrechte, Allgemeine Grundlagen – Grundrechte in Österreich, Entwicklungen – Rechtsschutz, facultas.wuv Universitätsverlag, Wien 2009; zitiert: *Autor* in *Heissl (Hg)*, Handbuch Menschenrechte (2009) [Rz] [Seite].
- Herzog, Felix*, Der Banker als Fahnder? Von der Verdachtsanzeige zur systematischen Verdachtsgewinnung – Entwicklungstendenzen der Geldwäschebekämpfung, WM 1996, 1753.

- Hofmann, Stefan / Walter, Bernhard*, Die Veräußerung Not leidender Kredite – aktives Risikomanagement der Bank im Spannungsverhältnis zwischen Bankgeheimnis und Datenschutz, WM 2004, 1566.
- Holliger-Hagmann, Eugénie*, Bankenhaftung: Vorsicht mit den Kundendaten, Schweizer Bank 07/2006, 42.
- Höllinger, Susanne*, Ab 1. Juli wird's ernst: Die neue EU-Zinsrichtlinie, VWT 2005 H 3, 48.
- Holoubek, Michael / Lang, Michael (Herausgeber)*, Rechtsschutz gegen staatliche Untätigkeit, Verlag Linde, Wien 2011; zitiert: *Autor* in *Holoubek/Lang (Hg)*, Rechtsschutz gegen staatliche Untätigkeit, [Seite].
- Hönel, Alexander / Raschauer, Nicolas / Wessely, Wolfgang*, Datenschutzrechtliche Fragestellungen im Zusammenhang mit klinischen Prüfungen, RdM 2006, 106.
- Iro, Gert Michael / Koziol, Helmut*, Allgemeine Bedingungen für Bankgeschäfte, Kommentar, Bank Verlag und Verlag Orac, Wien 2001 (Bankwissenschaftliche Schriftenreihe, Band 91); zitiert: *Autor* in *Iro/Koziol*, ABB-Kommentar (2001), [Ziffer, Rz].
- Iro, Gert Michael*, OGH: Unwirksame Klauseln in den Allgemeinen Geschäftsbedingungen der Banken, RdW 2003, 66.
- Jahnel, Dietmar*, Datenschutzkommission verfassungsrechtlich abgesichert – Zur Datenschutzgesetznovelle 1994, wbl 1994, 401.
- Jahnel, Dietmar*, Datenschutzrecht in der Praxis – Grundbegriffe, Zulässigkeit, Meldepflicht, Datensicherung, Rechtsschutz und Spamming, dbv-Verlag, Graz/Wien 2004; in: *Starl, Klaus (Herausgeber)*, Schriftenreihe „Arbeitsmaterialien zur Kanzleiorganisation“, Band V; zitiert: *Jahnel*, Datenschutzrecht in der Praxis, [Seite].
- Jahnel, Dietmar*, Handbuch Datenschutzrecht. Grundrecht auf Datenschutz, Zulässigkeitsprüfung, Betroffenenrechte, Rechtsschutz, Verlag Jan Sramek, Salzburg 2010; zitiert: *Jahnel*, Handbuch Datenschutzrecht [Rz].
- Jahnel, Dietmar*, Zur Aufhebung von § 14 DSG durch den Verfassungsgerichtshof, EDVuR 1994, 94.
- Jahnel, Dietmar / Siegwart, Stefan / Fercher, Natalie (Herausgeber)*, Aktuelle Fragen des Datenschutzrechtes, facultas.wuv Universitätsverlag, Wien 2007, zitiert: *Autor* in *Jahnel/Siewgart/Fercher (Hg)*, Aktuelle Fragen des Datenschutzrechtes, [Seite].
- Jirousek, Heinz*, Die Umsetzung des OECD-Standards der Amtshilfe in Österreich – das neue Amtshilfe-Durchführungsgesetz, SWI 2009, 488.
- Judt, Ewald / Koller, Monika*, Innovation im kartengestützten Zahlungsverkehr, ÖBA 2008, 250.

- Kastelitz, Markus*, Transatlantischer Datenschutzrechts-Dialog – ein Erfahrungsbericht, *jusIT* 2010, 180.
- Keiler, Stephan / Kristoferitsch, Hans*, Passagierdaten auf dem Flug in die USA. Neues Abkommen der EU mit den USA über die Weitergabe von Passagierdaten nach dem Urteil des EuGH verbundene Rs C-317/04, C-318/04, *ZVR* 2006, 484.
- Knörzer, Patrick*, Reform der EU-Zinsenbesteuerung: Auswirkungen auf Stiftungen, *SWI* 2009, 274.
- Knyrim, Rainer*, 25 Jahre Datenschutzrecht in Österreich – Bestandsaufnahme und Lösungsansätze für aktuelle Probleme, *MR* 2005, 415.
- Knyrim, Rainer*, Datenschutzrecht – Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmung, Outsourcen, Werben uvm, Verlag Manz, Wien 2003; zitiert: *Knyrim*, Datenschutzrecht, [Seite].
- Knyrim, Rainer*, Datenschutzrecht – Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmung, Outsourcen, Werben uvm, 2. vollständig überarbeitete Auflage, Verlag Manz, Wien 2012; zitiert: *Knyrim*, Datenschutzrecht², [Seite].
- Knyrim, Rainer*, Datenschutz bremsst Austausch in internationalen Konzernen, *DiePresse* 2006/44/01.
- Knyrim, Rainer*, Datenschutzrechts-Compliance in der Bank – Die wichtigsten datenschutzrechtlichen Themen für Kreditinstitute, *ÖBA* 2007, 476.
- Knyrim, Rainer*, Datenübermittlung in Drittländer: Standardvertragsklauseln der Europäischen Kommission, *AnwBl* 2001, 634.
- Knyrim, Rainer*, Neuerungen im Datenverkehr mit Drittländern, *ecolex* 2002, 466.
- Knyrim, Rainer*, Nochmals § 107 TKG 2003: Papierwerbung benachteiligt?, *ecolex* 2005, 257.
- Knyrim, Rainer*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, *ecolex* 2008, 1060.
- Knyrim, Rainer*, Zulässigkeit eines internationalen Datenverkehrs nach DSG 2000, *ecolex* 2002, 470.
- Knyrim, Rainer / Haidinger, Viktoria*, Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis, *RDV* 2005, 208.
- Kobrin, Stephen J.*, The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance (November 2002) = <http://knowledge.wharton.upenn.edu/papers/1080.pdf> (Stand: 25.07.2012).
- Korinek, Stephan*, Das Transparenzgebot des § 6 Abs 3 KSchG, *JB1* 1999, 149.

- Kotschy, Waltraut*, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 307.
- Koziol, Helmut*, OGH 19.11.2002, 4 Ob 179/02f, ÖBA 2003, 141.
- Koziol, Helmut*, OGH 15.12.2005, 6 Ob 275/05t, ÖBA 2006, 530.
- Koziol, Helmut (Glossar: Rummel, Peter)*, OGH 20.03.2007, 4 Ob 221/06p – Zur Unwirksamkeit von Klauseln in den AGB einer Bank, ÖBA 2007, 981.
- Kunnert, Gerhard*, Das „gläserne Auto“ – Überlegungen aus datenschutzrechtlicher Sicht, ZVR 2002, 219.
- Kurioses & Wissenswertes*, SWIFT-Abkommen zum Transfer von Finanzdaten in Kraft getreten, jusIT 2010, 162.
- Lafite, Wolfgang / Vondrak, Philip / Gruber, Philip*, Spiel mir das Lied vom Tod, Bankgeheimnis!, ecolex 2010, 82.
- Lafite, Wolfgang / Vondrak, Philip / Gruber, Philip*, Quo vadis Bankgeheimnis? Möglichkeiten und Grenzen bei der Umsetzung des OECD-Standards betreffend Informationsaustausch in Steuersachen, ecolex 2009, 573.
- Lehofer, Hans Peter*, VfGH: EU-Grundrechte-Charta als Prüfungsmaßstab, ÖJZ 2012, 433.
- Leissler, Günther*, Der neue europäische Datenschutzrahmen, ecolex 2012, 268.
- Leissler, Günther*, Und die Daten fließen über den Atlantik..., ecolex 2007, 747.
- Lengauer, Alina*, Union Aktuell, ZfRV 2008, 148.
- Lenz, Carl Otto / Borchardt, Klaus-Dieter (Herausgeber)*, EU-Verträge (2010), 5. Auflage, Verlag Linde ua, Wien 2010; zitiert: Autor in *Lenz/Borchardt*, EU-Verträge⁵, [Art] [Rz].
- Leupold, Petra / Ramharter, Martin*, Die Verletzung der Pflicht zur Warnung vor mangelnder Kreditwürdigkeit nach dem Verbraucherkreditgesetz – Europarechtliche Grundlagen und zivilrechtliche Konsequenzen, ÖBA 2011, 469.
- Meincke, Eberhard*, Geheimhaltungspflichten im Wirtschaftsrecht, WM 1998, 749.
- Merten, Detlef / Papier, Hans-Jürgen (Herausgeber)*, Handbuch der Grundrechte in Deutschland und Europa, Band VII/1 Grundrechte in Österreich (in Koordination mit *Heinz Schäffer*), Verlag Manz ua, Wien 2009; zitiert: Autor, Titel des Kapitels, in: *Merten/Papier*, HGR VII/1, [§] [Rz].
- Mütsch, Burkard*, Kreditwirtschaftlich wichtige Vorhaben der EU, Kreditwesen 1997, 1058.
- Nobbe, Gerd*, Bankgeheimnis, Datenschutz und Abtretung von Darlehensforderungen, WM 2005, 1537.

- Oberndorfer, Paul / Trybus, Peter*, Informationsverbundsysteme und Datenschutz am Beispiel europäischer Bankengruppen, *ÖZW* 2007, 14.
- Öhlinger, Theo*, Verfassungsrecht, 8., überarbeitete Auflage, facultas.wuv Universitätsverlag, Wien 2009; zitiert: *Öhlinger*, Verfassungsrecht⁸ [Rz].
- Österreichische Juristenkommission*, Grundrechte im Europa der Zukunft, Verlag Linde, Wien 2010 (= Kritik und Fortschritt im Rechtsstaat, Band 36); zitiert: *Autor* in *ÖJK (Hg)*, Grundrechte im Europa der Zukunft, [Seite].
- Pauly, Daniel A. / Ritzer, Christoph*, Datenschutz-Novellen: Herausforderungen für die Finanzbranche, *WM* 2010, 8.
- Pollirer, Hans-Jürgen / Weiss, Ernst M. / Knyrim, Rainer (Hrsg)*, Datenschutzgesetz 2000 (DSG 2000) samt ausführlichen Erläuterungen, Manzsche Gesetzausgaben, Sonderausgabe Nr 115, Wien 2010; zitiert: *Pollirer/Weiss/Knyrim*, DSG (2010) [§] [Anm].
- Potyka, Matthias*, Die Hauptversammlung nach dem AktRÄG 2009. Einführung verschiedener Formen der elektronischen Teilnahme und des Nachweisstichtagssystems, *CFOaktuell* 2009, 174.
- Priesemann, Johannes*, Regulierung und Überwachung im einheitlichen Zahlungsverkehrsmarkt, *ÖBA* 2006, 855.
- Rabe, Stephan F.*, Kreditwirtschaftlich wichtige Vorhaben der EU, *Kreditwesen* 1999, 1209.
- Raschauer, Bernhard*, Allgemeines Verwaltungsrecht, 3., vollständig überarbeitete Auflage, Verlag Springer, Wien ua 2009; zitiert: *Raschauer*, Allgemeines Verwaltungsrecht³, [Rz].
- Raschauer, Bernhard*, Bankenaufsicht (Skriptum)⁸ (2012), [Seite].
- Riegler, Marco / Trappitsch, Michael*, Datenübermittlung und Zustimmungproblematik im Datenschutzgesetz, *RdW* 2005, 341.
- Rinze, Jens / Heda, Klaudius*, Non-Performing Loan und Verbriefungs-Transaktionen: Bankgeheimnis, Datenschutz, § 203 StGB und Abtretung – zugleich eine Besprechung des Urteils des OLG Frankfurt a.M. vom 25. Mai 2004 (= *WM* 2004, 1386), *WM* 2004, 1557.
- Roth, Günter / Fitz, Hanns*, Anonymität, Identitätsfeststellung und Bankgeheimnis, *ÖBA* 1996, 409.
- Schobel, Thomas*, Verletzung von Geheimhaltungspflichten durch Banken, *ÖBA* 2004, 8.
- Schütz, Oliver / Waldherr, Markus*, Die Auslagerung bankgeschäftlicher Tätigkeiten aus bankaufsichtsrechtlicher Sicht (Outsourcing), *ÖBA* 2007, 138.

- Sedef, Arzu*, 1. Österreichischer IT-Rechtstag – ein Tagungsbericht, MR 2007, 241.
- Sedlak, Michael*, Schaffung des europäischen Zahlungsraumes – SEPA und das Zahlungsdienstegesetz, NetV 2010, 7.
- Sonntag, Michael*, Einführung in das Internetrecht – Rechtsgrundlagen für Informatiker, Verlag Linde, Wien 2009; zitiert: *Sonntag*, Einführung in das Internetrecht, [Seite].
- Stadler, Gerhard*, Das österreichische Datenschutzgesetz als Markstein der Verfassungspolitik und des Informationsrechtes, JBl 1979, 358.
- Tretter, Hannes*, Der digital bewegte Mensch. Europäische Präsidentenkonferenz 2010, AnwBl 2010, 165.
- Ulmer, Peter / Brandner, Hans Erich / Hensen, Horst-Diether / Schmidt, Harry*, AGB Gesetz, Kommentar zum Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 9. umfassend überarbeitete Auflage, Verlag Dr. Otto Schmidt, Köln 2001; zitiert: *Autor* in *Ulmer/Brandner/Hensen*, AGB-Gesetz⁹ (2001), [§] [Rz].
- Urbantschitsch, Wolfgang / Hofer, Edith*, Terrorismusbekämpfung, ecolex 2010, 917.
- Urlesberger, Franz*, Europarecht: Das Neueste auf einen Blick, wbl 2003, 118.
- Urlesberger, Franz*, Europarecht: Das Neueste auf einen Blick, wbl 2007, 224.
- Urlesberger, Franz*, Europarecht: Das Neueste auf einen Blick, wbl 2010, 177.
- Urtz, Christoph*, VwGH-Rechtsprechung: Das österreichische Bankgeheimnis schützt deutsche Steuerstraftäter!, GeS 2007, 21.
- Volk, Tobias*, Outsourcing der Raterstellung im Lichte des deutschen Datenschutzes und Bankgeheimnisses, ÖBA 2009, 372.
- Wagner, Dietmar / Eigner, Wolfgang*, Aufsichtsrechtliche Aspekte der Zahlungsdiensterichtlinie, ÖBA 2008, 633.
- Walter, Robert / Mayer, Heinz / Kucsko-Stadlmayer, Gabriele*, Grundriss des österreichischen Bundesverfassungsrechts auf Grundlage der von *Walter/Mayer* gestalteten 1. bis 9. Auflage, 10., durchgesehene und ergänzte Auflage, Verlag Manz, Wien 2007; zitiert: *Walter/Mayer/Kucsko-Stadlmayer*, Verfassungsrecht¹⁰ [Rz] [Seite].
- Weissel, Georg*, Zur Anwendung von § 7 VKrG, ÖBA 2012, 302.
- Wendehorst, Christiane / Zöchling-Jud, Brigitta*, Verbraucherkreditrecht – VerbraucherkreditG und ABGB-Darlehensbestimmungen, Verlag Manz, Wien 2010; zitiert: *Autor* in *Wendehorst/Zöchling-Jud*, Verbraucherkreditrecht (2010), [§, Rz].
- Wittmann, Heinz*, Die Datenschutzkonvention des Europarates, EDVuR 1989, 96.
- Wolf, Manfred / Horn, Norbert / Lindacher, Walter F.*, AGB-Gesetz – Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, Kommentar, 4., völlig

überarbeitete Auflage, C. H. Beck'sche Verlagsbuchhandlung, München 1999; zitiert:
Autor in Wolf/Horn/Lindacher, AGB Gesetz⁴ (1999) [§] [Rz].
*Zubrod, Andreas, Automatisierter Abruf von Kontoinformationen nach § 24c KWG –
Rechtliche Voraussetzungen und Grenzen, WM 2003, 1210.*

Zusätzlich habe ich mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und
soweit notwendig ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt.

Verwendete Webseiten

<http://register.consilium.europa.eu>
<http://www.bmf.gv.at>
<http://www.bundesfinanzministerium.de>
<http://www.bundeskanzleramt.at> (entspricht <http://www.bka.gv.at>)
<http://www.bzst.de>
<http://www.coe.int> (vgl insb <http://www.conventions.coe.int> und <http://www.echr.coe.int>)
<http://www.curia.europa.eu>
<http://www.derstandard.at>
<http://www.diepresse.com>
<http://www.dsk.gv.at>
<http://www.ejustice.just.fgov.be/cgi/summary.pl>
<http://www.eur-lex.europa.eu>
<http://www.europarl.europa.eu>
<http://www.europoljsb.consilium.europa.eu>
<http://www.export.gov/safeharbor>
<http://www.fma.gv.at>
<http://www.heise.de>
<http://www.legilux.public.lu>
<http://www.nzz.ch>
<http://www.oecd-ilibrary.org>
<http://www.oenb.at>
<http://www.parlament.gv.at>
<http://www.ris.bka.gv.at>
<http://www.schufa.de>
<http://www.sif.admin.ch>
<http://www.spiegel.de>
<http://www.swift.com>
<http://www.videoportal.sf.tv>
<http://www.wirtschaftsblatt.at>
<http://zmr.bmi.gv.at>

Judikaturverzeichnis

Gericht	Datum	Aktenzahl	Fundstelle	Fundstelle 2
BVerfG	13.06.2007	1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05	www.bundesverfassungsgericht.de/entscheidungen.html	
DSK	18.05.2000	120.616/16-DSK/00	RIS-Justiz	
DSK	21.09.2001	K095.014/016-DSK/2001	RIS-Justiz	
DSK	23.11.2001	K095.014/021-DSK/2001	RIS-Justiz	
DSK	03.12.2002	K120.804/016-DSK/2002	RIS-Justiz	
DSK	11.07.2003	K120.629/002-DSK/2003	RIS-Justiz	
DSK	25.06.2004	K120.877/0017-DSK/2004	RIS-Justiz	
DSK	07.12.2004	K120.938/0003-DSK/2004	RIS-Justiz	
DSK	01.02.2005	K120.637/0001-DSK/2005	RIS-Justiz	
DSG	01.02.2005	K500.974-033/0002-DVR/2005	RIS-Justiz	
DSK	07.06.2005	K121.006/0007-DSK/2005	RIS-Justiz	
DSK	29.11.2005	K211.593/0011-DSK/2005	RIS-Justiz	
DSK	05.04.2006	K121.136/0004-DSK/2006	RIS-Justiz	
DSK	07.09.2006	K202.047/0009-DSK/2006	RIS-Justiz	
DSK	21.03.2007	K600.014-010/0002-DVR/2007	RIS-Justiz	
DSK	27.04.2007	K211.797/0004-DSK/2007	RIS-Justiz	
DSK	07.05.2007	K211.773/0009-DSK/2007	RIS-Justiz	
DSK	10.08.2007	K121.275/0007-DSK/2007	RIS-Justiz	
DSK	10.08.2007	K121.276/0014-DSK/2007	RIS-Justiz	
DSK	12.12.2007	K600.033-018/0002-DVR/2007	RIS-Justiz	
DSK	22.10.2008	K121.386/0009-DSK/2008	RIS-Justiz	
DSK	25.02.2009	K121.394/0006-DSK/2009	RIS-Justiz	
DSK	19.06.2009	K121.494/0013-DSK/2009	RIS-Justiz	
DSK	18.09.2009	K121.518/0005-DSK/2009	RIS-Justiz	
DSK	14.04.2010	K121.564/0006-DSK/2010	RIS-Justiz	
DSK	12.05.2010	K202.088/0003-DSK/2010	RIS-Justiz	
DSK	27.08.2010	K121.599/0014-DSK/2010	RIS-Justiz	
DSK	24.11.2010	K121.646/0011-DSK/2010	RIS-Justiz	
DSK	18.05.2011	K121.667/0012-DSK/2011	RIS-Justiz	
EuGH	30.05.2006	Rs C-317/04 und C-318/04	ZVR 2006, 484	
EuGH	10.02.2009	Rs C-301/06	MR 2009, 3	
EuGH	09.03.2010	Rs C-518/07		
EuGH	09.11.2010	Rs C-92/09 und C-93/09	ÖJZ 2011, 955	
EuGH	18.05.2011	Rs C-614/10	B des EuGH-Präs.	
EuGH	07.07.2011	Rs C-614/10	B des EuGH-Präs.	

OGH	29.01.1997	7 Ob 2299/96f	ÖJZ 1997, 632	KRES 10/62a; ÖBA 1997, 632
OGH	22.03.2001	4 Ob 28/01y	Ecolex 2001, 147	RdW 2001, 531; ÖBA 2001, 645
OGH	13.09.2001	6 Ob 16/01y	RIS-Justiz	
OGH	19.11.2002	4 Ob 179/02f	VRInfo 2003 H 1, 4	KRES 3/113
OGH	11.08.2005	4 Ob 88/05b	RIS-Justiz	
OGH	15.12.2005	6 Ob 275/05t	ZIK 2006, 68	RdW 2006, 212
OGH	22.02.2006	9 Ob 12/06i	RIS-Justiz	
OGH	04.05.2006	9 Ob 15/05d	RIS-Justiz	
OGH	17.01.2007	7 Ob 131/06z	RIS-Justiz	
OGH	17.01.2007	7 Ob 140/06y	RIS-Justiz	
OGH	17.01.2007	7 Ob 173/06a	RIS-Justiz	
OGH	20.03.2007	4 Ob 221/06p	KRES 1d/95	
OGH	27.03.2007	1 Ob 241/06g	RIS-Justiz	
OGH	05.06.2007	10 Ob 67/06k	RIS-Justiz	
OGH	07.11.2007	6 Ob 110/07f	RIS-Justiz	
OGH	11.03.2008	4 Ob 5/08a	RIS-Justiz	
OGH	01.10.2008	6 Ob 195/08g	RIS-Justiz	
OGH	06.11.2008	6 Ob 220/08h	RIS-Justiz	
OGH	28.01.2009	10 Ob 70/07b	RIS-Justiz	
OGH	02.04.2009	8 Ob 119/08w	RIS-Justiz	
OGH	16.04.2009	2 Ob 137/08y	RIS-Justiz	
OGH	13.05.2009	7 Ob 230/08m	RIS-Justiz	
OGH	19.05.2009	3 Ob 12/09z	RIS-Justiz	
OGH	18.09.2009	6 Ob 128/09f	RIS-Justiz	
OGH	12.11.2009	6 Ob 156/09y	RIS-Justiz	
OGH	17.12.2009	6 Ob 247/08d	RIS-Justiz	
OGH	17.03.2010	7 Ob 13/10b	RIS-Justiz	
OGH	17.03.2010	7 Ob 15/10x	RIS-Justiz	
OGH	15.04.2010	6 Ob 41/10p	RIS-Justiz	
OGH	22.04.2010	2 Ob 1/09z	RIS-Justiz	
OGH	19.05.2010	6 Ob 2/10b	ÖBA 2010, 853	
OGH	27.05.2010	5 Ob 64/10p	RIS-Justiz	
OGH	22.10.2010	7 Ob 109/09v	RIS-Justiz	
OGH	23.11.2010	1 Ob 164/10i	RIS-Justiz	
OGH	11.05.2011	7 Ob 173/10g	RIS-Justiz	
OGH	07.06.2011	5 Ob 42/11d	RIS-Justiz	
OGH	12.10.2011	7 Ob 68/11t	RIS-Justiz	
OLG Wien	17.04.2002	1 R 229/01f	VRInfo 2002 H 5a, 1	
VfGH	07.12.1994	B 331/94	RIS-Justiz	
VfGH	11.03.2004	V 126/03	RIS-Justiz	
VfGH	06.10.2006	G 151/05	RIS-Justiz	
VfGH	04.12.2006	V 22/05	RIS-Justiz	

VfGH	17.12.2009	B 504/09	RIS-Justiz	
VfGH	14.03.2012	U 466/11 und U 1836/11	RIS-Justiz	
VwGH	26.07.2006	2004/14/0022	RIS-Justiz	

Deutsche Zusammenfassung

Die vorliegende Dissertation behandelt den automatischen Datenaustausch im Bereich der Finanzdienstleistungen. Ausgehend von den Artt 8 ff der RL 2003/48/EG, welche die automatische Auskunftserteilung sowie Übergangsbestimmungen für Belgien, Luxemburg und Österreich vorsehen, werden grundlegende relevante Begriffe und das Verhältnis zum österr Bankgeheimnis analysiert.

Im Kapitel „Informationsverbundsysteme“ werden anschauliche Beispiele jederzeit verfügbarer österr Datenspeichersysteme sowie deren deutsche Pendant erörtert: „Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten“, „Kleinkreditevidenz (Konsumentenkreditevidenz) zum Zweck des Gläubigerschutzes und der Risikominimierung“ und andere Bonitätsdatenbanken bilden den Schwerpunkt dieses Abschnittes und zeigen, dass gesetzliche Regelungen für die Zulässigkeit von Bonitätsdatenbanken anzustreben sind. Daran schließen sich datenschutzrechtliche Überlegungen zur Zulässigkeit einer nationalen und internationalen Datenverwendung bzw -verarbeitung iSd Datenschutzrichtlinie RL 1995/46/EG – hierzu finden sich auch praktische Prüfungsschritte zur Zulässigkeit. Unterschiedliche Terminologien österr und europäischer Regelungen sind für das Verständnis dieses Bereiches jedoch hinderlich und sollten bereinigt werden. Auch die Datenschutzangemessenheitsverordnung (DSAV) wurde erst 2013 aktualisiert.

Schließlich wird ein Überblick zu den bedeutsamen nationalen und europäischen grundrechtlichen Regelungen des Datenschutzes mit Schwerpunkt auf die aus der Charta der Grundrechte der Europäischen Union erwachsenden Rechte gegeben. In den Schlussfolgerungen wird konkreter Handlungsbedarf (insb das österr DSG betreffend) zur weiteren Rechtsentwicklung aufgezeigt.

Diese Dissertation soll datenschutzrechtliche Fragestellungen im Bereich der Finanzdienstleistungen klären und vor allem notwendige Änderungen des Datenschutzrechtes benennen. Um eine fundierte Kenntnis des Datenschutzrechtes im Bereich der Finanzdienstleistungen zu festigen, sind auch Schilderungen zum SWIFT-Abkommen, wodurch täglich mehrere Millionen standardisierte Finanznachrichten abgewickelt werden

können, zum Verhältnis zu Geldwäsche- und Terrorismusbekämpfungsnormen, EDI und SEPA notwendige Voraussetzung. Die Fülle an derzeit in Diskussion befindlichen Reformen (vgl etwa die „Datenschutz-Verordnung“) weist auf die Komplexität datenschutzrechtlicher Regelungen hin und ermöglicht einen Blick über den Bereich der Finanzdienstleistungen hinaus.

English Abstract

This doctoral thesis deals with „automatic data exchange in the field of financial services“. Starting with Articles 8 et seq of the Council directive 2003/48/EC, which set the automatic exchange of information as well as a transitional period for Belgium, Luxembourg and Austria, fundamental terms and their relationship to the Austrian banking secrecy are analysed.

In the chapter “Informationsverbundsysteme” demonstrative examples of Austrian databases providing access at any time as well as their German counterparts are presented: The focus is laid on the Austrian databases “Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten”, “Kleinkreditevidenz (Konsumentenkreditevidenz) zum Zweck des Gläubigerschutzes und der Risikominimierung” as well as other credit rating databases. They prove that statutory rules are necessary. The following part reflects on data protection in regard to admissibility of national or international data processing within the meaning of the Directive 1995/46/EC of the European Parliament and the Council - practical examination steps concerning the admissibility are given. Differing terminology of Austrian and European regulations in this field can lead to misunderstandings and should be eliminated. Furthermore, it was only after more than ten years, that the Austrian regulation on the adequate protection of data (“Datenschutzangemessenheitsverordnung (DSAV)”) has been updated.

Finally the thesis gives an overview on the most important national and European fundamental rights in the field of data protection, especially the rights defined in the Charter of Fundamental Rights of the European Union. The conclusions show concrete need of action (in particular concerning the Austrian data protection act) in order to develop the law.

The thesis aims to clarify data protection problems in the field of financial services and names necessary amendments of data protection law. To deepen knowledge of data protection law in the field of financial services, the thesis also discusses the SWIFT-Agreement, which allows to exchange millions of standardised financial messages every day, its relationship to money laundering and counter-terrorist regulations, EDI (Electronic Data Interchange) and SEPA (Single European Payment Area). The abundance of reforms in discussion (eg “data

protection regulation”) shows the complexity of data protection provisions and allows a view beyond the field of financial services.

Lebenslauf

Name Andreas Fussenegger
Adresse Bürglegasse 24a, 6850 Dornbirn
Telefon +43 650 2698702
Staatsangehörigkeit Österreich
Geburtsdatum 08.07.1987 (in Feldkirch)



SCHUL- UND BERUFSBILDUNG

2009 – dato Doktratsstudium der Rechtswissenschaften an der Universität Wien
2009 – 2010 LL.M.-Studium an der Universität Wien, Europäisches und Internationales Wirtschaftsrecht, Abschluss mit Master of Laws (LL.M.)
01/2008 – 06/2008 Auslandsstudium im Rahmen des Erasmus-Programms an der Université de Franche-Comté, Besançon (Frankreich)
2005 – 2009 Diplomstudium der Rechtswissenschaften an der Universität Wien, Abschluss mit Mag. iur.
1997 – 2005 Bundesrealgymnasium Dornbirn Schoren, Abschluss mit der AHS-Matura mit ausgezeichnetem Erfolg

BERUFSERFAHRUNG MIT BEDEUTUNG FÜR WISSENSCHAFTLICHEN WERDEGANG

Seit 10/2012 Rechtsanwaltsanwärter
07/2010 – 09/2012 Gerichtsjahr in Vorarlberg (mit Unterbrechungen)
Sommer 2009 Praktikum bei Rechtsanwaltskanzlei in Wien
Sommer 2008 Außenhandelsstelle Zagreb der WKÖ (Österreichische Botschaft in Kroatien, Abteilung Wirtschaft)