

DATENSCHUTZ VERSUS KREDITSCHUTZ
ÜBER DIE ZULÄSSIGKEIT VON BONITÄTSAUSKÜNFTEN
AUS DATENBANKEN IM PRIVAT- UND FIRMENKUNDENSEGMENT

DISSERTATION

eingereicht

an der

RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER
UNIVERSITÄT WIEN

zur Erlangung des akademischen Grades

DOCTOR IURIS

von **Mag. Thomas PAWLIK**

im April 2009

Erstbegutachter: O. Univ.-Prof. Dr. Bernhard RASCHAUER

Zweitbegutachter: Ao. Univ.-Prof. Mag. Dr. Christian M. PISKA

INHALTSVERZEICHNIS

1.	Einleitung	11
2.	Zur Entstehung des Datenschutzes	13
2.1.	Die Sphärentheorie	13
2.2.	Die Mosaiktheorie	14
2.3.	Das rollentheoretische Konzept	14
2.4.	Der Begriff „privacy“	16
2.5.	Die vier Generationen des Datenschutzes	17
2.6.	Datenschutz in der Europäischen Union	19
2.7.	Datenschutz in Österreich	27
2.7.1.	Die Entstehung des Datenschutzes in Österreich	27
2.7.2.	Das Grundrecht auf Datenschutz	30
2.7.2.1.	Arten von personenbezogenen Daten	36
2.7.2.2.	Beschränkungen des Grundrechts	37
2.7.3.	Österreichisches Verfassungsrecht und EMRK	41
3.	Bonität/Kreditwürdigkeit	47
3.1.	Das Kreditrisiko	47
3.2.	Die Kreditprüfung/Kreditanalyse	48
3.3.	Die Offenlegungspflichten von Kapitalgesellschaften	50
3.4.	Die „Offenlegungspflichten“ von Auskunftsteilen	55
4.	Wirtschaftliche Aspekte	57
5.	Die Prüfung der Zulässigkeit der Datenermittlung	61
5.1.	Der Begriff von „Treu und Glauben“	62
5.2.	Der anerkannte Zweck	64
5.3.	Die sachliche Richtigkeit	66
5.4.	Die Aufbewahrungsdauer	66
6.	Die Zulässigkeit der Datenverarbeitung	69
6.1.	Zweck und Inhalt bestimmt	69
6.2.	Die schutzwürdigen Geheimhaltungsinteressen	70
6.2.1.	Die gesetzliche Ermächtigung oder Verpflichtung	72
6.2.2.	Die Zustimmung	73
6.3.	Die Zulässigkeit der Datenübermittlung	80
6.3.1.	Die gesetzliche Zuständigkeit oder rechtliche Befugnis	84
6.3.2.	Die schutzwürdigen Geheimhaltungsinteressen	85
7.	Die Beteiligten im Datenschutzgesetz	91
7.1.	Der Betroffene („Grundrechtsträger“)	91
7.2.	Der Auftraggeber („Grundrechtsverpflichtete“)	92
7.3.	Der Dienstleister	94
8.	Das EuGH Urteil im Fall „Lindqvist“	101
9.	Das EuGH Urteil im Fall „Asnef-Equifax/Ausbanc“	103
10.	Der Kreditschutzverband von 1870 (KSV)	107
10.1.	Die Bonitäts-/Wirtschaftsauskunft im Allgemeinen	109
10.2.	KSV Wirtschaftsdatenbank	112
10.2.1.	Die wichtigsten Daten und Fakten in der KSV Wirtschaftsdatenbank	121
10.2.2.	Ratingkennzahlen und ihre Bedeutung	123
10.2.2.1.	KSV Neugründer Score	124
10.2.2.2.	Berechnungsmodell des KSV-Ratings im Detail	125
10.2.2.3.	Berechnungsmodell kleine Bilanzen	126
10.2.2.4.	Berechnungsmodell Strukturdaten (weiche Faktoren)	128

10.2.3.	Rechtliche Beurteilung	129
10.3.	Die KKE (KonsumentenKreditEvidenz) Datenbank	132
10.3.1.	Rechtliche Beurteilung	142
10.4.	Exkurs: Sonderfall Grosskreditevidenz.....	144
10.5.	Die UKV Datenbank – Liste der Unerwünschten KontoVerbindungen	145
10.5.1.	Das OGH Urteil 6 Ob 275/05t vom 15.12.2005	150
10.5.2.	Das Urteil OGH 1 Ob 38/88 vom 28.9.1988.....	153
10.5.3.	Das Urteil LG ZRS Wien 9 Cg 216/99x vom 21.2.2000	154
10.5.4.	Rechtliche Beurteilung	155
10.6.	Die WKE – WarenKreditEvidenz - Datenbank	157
10.6.1.	Rechtliche Beurteilung	166
11.	Deltavista GmbH Österreich	167
11.1.	Rechtliche Beurteilung	171
12.	Datengeheimnis (§ 15 DSG 2000)	174
12.1.	Umfang der Verschwiegenheitspflicht.....	175
12.2.	Verpflichtungserklärung.....	176
12.3.	Bruch der Verschwiegenheitspflicht	177
13.	Offenlegungs- und Informationspflichten des Auftraggebers.....	178
14.	Die Rechte des Betroffenen.....	181
14.1.	Das Recht auf Auskunft	183
14.2.	Recht auf Richtigstellung oder Löschung	200
14.3.	Widerspruchsrecht.....	204
14.3.1.	Das Urteil OGH 6 Ob 195/08g.....	206
15.	Sonderbestimmungen	209
15.1.	Automatisierte Einzelentscheidungen	209
15.2.	Data-mining, Data-warehousing	210
15.3.	Informationsverbundsystem	212
16.	Rechtsschutz.....	214
17.	Strafbestimmungen.....	220
17.1.	Verwaltungsstrafrechtliche Bestimmungen	220
17.2.	Zivilrechtliche Bestimmungen	221
17.2.1.	Schadenersatz	221
17.2.2.	Das Urteil LGZ Wien 53 Cg 106/07h vom 15.2.2008.....	224
17.2.3.	Weitere zivilrechtliche Bestimmungen	226
17.3.	Strafrechtliche Bestimmungen	227
18.	Exkurs - Das Bankgeheimnis	229
18.1.	Die Bankauskunft	248
19.	Das Zentrale Melderegister (ZMR).....	254
20.	Schlussbemerkungen	257

ANHANG I – Das DSG 2000

ANHANG II – Die DS-RL 95/46/EU

ABKÜRZUNGSVERZEICHNIS

aA	andere Ansicht
aaO	an anderer Ordnung
AB	Ausschussbericht
ABB	Allgemeine Geschäftsbedingungen für Bankgeschäfte
ABGB	Allgemein Bürgerliches Gesetzbuch
ABl	Amtsblatt
aM	andere Meinung
ABIEG	Amtsblatt der Europäischen Gemeinschaft
Abs	Absatz
AktG	Aktiengesetz
Anm	Anmerkung
Appl	Application (Nummer/Jahr)
Art	Artikel
AVG	Allgemeines Verwaltungsverfahrensgesetz
BAO	Bundesabgabenordnung
BDSG	Bundesdatenschutzgesetz (D)
BGB	Bürgerliches Gesetzbuch (D)
BGBI	Bundesgesetzblatt (Ö)
BGH	Bundesgerichtshof (D)
BGHZ	Sammlung der Entscheidungen des BGH in Zivilrechtssachen
BlgNr	Beilagen zur Nationalratsperiode
BVerfG	Bundesverfassungsgericht (D)
B-VG	Bundesverfassungsgesetz (Ö)
BvR	Aktenzeichen einer Verfassungsbeschwerde beim Bundesverfassungsgericht (D)

BVR	Österreichisches Bankvertragsrecht
BWG	Bankwesengesetz/ Bankwissenschaftliche Gesellschaft (Schriftenreihe)
bzw	beziehungsweise
CR	Computer und Recht (Zeitschrift D)
dh	das heißt
Dipl.arbeit	Diplomarbeit
Diss	Dissertation
DSG	Datenschutzgesetz (Ö)
DSB	Datenschutzbericht (Ö)
DSK	Datenschutzkommission (Ö)
DS-RL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („ <i>Datenschutzrichtlinie</i> “)
DuD	Datenschutz und Datensicherheit (Zeitschrift D)
DVR	Datenverarbeitungsregister
E	Entscheidung
EB	Erläuternde Bemerkungen
ecolex	Fachzeitschrift für Wirtschaftsrecht
EDVuR	EDV und Recht (Zeitschrift)
EGMR	Europäischer Gerichtshof für Menschenrechte
EKIS	Elektronisches Kriminalpolizeiliches Informationssystem
EMRK	Europäische Menschenrechtskonvention
EO	Exekutionsordnung (Ö)
Erk	Erkenntnis
ErläutRV	Erläuterungen zur Regierungsvorlage
etc	et cetera

EU	Europäische Union
EuGH	Europäischer Gerichtshof
EvBl	Evidenzblätter der Rechtsmittelentscheidungen (ständiger Bestand der ÖJZ)
EWiR	Entscheidungen zum Wirtschaftsrecht (Zeitschrift)
EWS	Europäisches Wirtschafts- und Steuerrecht (Zeitschrift)
ff	fortfolgende
FinStrG	Finanzstrafgesetz
FMA	Finanzmarktaufsicht
FN	Fußnote
FS	Festschrift
gem	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz (D)
ggf	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GP	Gesetzgebungsperiode
GR	Grundrecht(e)
GZ	Geschäftszahl Österreichische Allgemeine Gerichtszeitung
hA	herrschende Ansicht
hL	herrschende Lehre
hM	herrschende Meinung
Hrsg	Herausgeber
idF	in der Fassung
idgF	in der geltenden Fassung
idR	in der Regel

iSd	im Sinne des
iSv	im Sinne von
iVm	in Verbindung mit
JA	Justizausschuss
JAP	Juristische Ausbildung u. Praxisvorbereitung (Zeitschrift)
JB1	juristische Blätter
JN	Jurisdiktionsnorm
JZ	Juristenzeitung
KaKuG	Krankenanstalten- und Kuranstaltengesetz
KO	Konkursordnung
Komm	Kommentar
KschG	Konsumentenschutzgesetz
KSV	Kreditschutzverband von 1870
KWG	Kreditwesengesetz
leg cit	legis citatae
lit	litera
LG	Landesgericht
LGZ	Landesgericht für Zivilrechtssachen
mE	meines Erachtens
MR	Medien und Recht (Zeitschrift)
MRK	Europäische Menschenrechtskonvention
mwN	mit weiteren Nachweisen
nF	neue Fassung
NJW	Neue Juristische Wochenschrift (D)
Nr	Nummer
NVwZ	Neue Zeitung für Verwaltungsrecht (D)

NZ	Notariatszeitung
Oä	oder ähnliches
OeNB	Österreichische Nationalbank
OGH	Oberster Gerichtshof
ÖBA	Österreichisches Bankarchiv
ÖBl	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht
ÖJZ	Österreichische Juristenzeitung
OLG	Oberlandesgericht
ÖStZB	Beilage zur österreichischen Steuerzeitung
Österr BVfR	Österreichisches Bundesverfassungsrecht
ÖZW	Österreichische Zeitschrift für Wirtschaftsrecht
RAO	Rechtsanwaltsordnung
RdW	Recht der Wirtschaft (Zeitschrift)
Ris	Rechtsinformationssystem
RL	Richtlinie
Rn	Randnummer
Rsp	Rechtssprechung
RV	Regierungsvorlage
RWZ	Zeitschrift für Recht und Rechnungswesen
Rz	Randzahl
Slg	Sammlung
stRsp	ständige Rechtssprechung
StGB	Strafgesetzbuch (Ö)
StPO	Strafprozessordnung (Ö)
TKG	Telekommunikationsgesetz

ua	unter anderem
uä	und ähnliches(s)
UGB	Unternehmensgesetzbuch (Ö)
UStG	Umsatzsteuergesetz
usw	und so weiter
uU	unter Umständen
UVS	Unabhängiger Verwaltungssenat (Ö)
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und Beschlüsse des VfGH
vgl	vergleiche
VO	Verordnung
VStG	Verwaltungsstrafgesetz
VwGH	Verwaltungsgerichtshof
VwSlg	Sammlung der Erkenntnisse und Beschlüsse des VwGH
wbl	wirtschaftliche Blätter
WM	Wertpapier Mitteilungen Zeitschrift für Wirtschafts- und Bankrecht
WuR	Zeitschrift für Wirtschaft und Recht
Z	Ziffer
zB	zum Beispiel
ZfV(B)	Zeitschrift für Verwaltung; (=Judikaturbeilage)
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZHR	Zeitschrift für das gesamte Handels- und Wirtschaftsrecht
ZIK	Zeitschrift für Insolvenzrecht und Kreditschutz
Zl	Zahl
ZPO	Zivilprozessordnung (Ö)
zT	zum Teil

1. Einleitung

Vielen Konsumenten ist nicht bewusst, dass sie bei jedem Kredit, bei jedem Handyvertrag, bei jeder Bestellung in einem Versandhaus Spuren hinterlassen, die eifrig gesammelt und verarbeitet werden. Erst wenn ihnen eine Bank wegen angeblich mangelnder Bonität einen Kredit verweigert oder es keinen Vertrag von einem Mobilfunkbetreiber gibt, werden Verbraucher hellhörig.¹

Die Ursprünge für die vermeintlichen "Bonitäts-Probleme" von Dr. Anton K. lagen vor ein paar Monaten bei seinem Wochenendhaus am Attersee. Er wurde unbemerkt dabei gefilmt, wie er fünf Zeitungen neben einen Altpapiercontainer gelegt hat, weil der Papiercontainer hoffnungslos überfüllt war. Wenig später forderte eine private Sicherheitsfirma von Herrn Dr. K. schriftlich € 100 Strafe wegen Verletzung des Abfallwirtschaftsgesetzes. Eine rechtlich kaum haltbare Vorgehensweise, doch nachdem der "Altpapier-Sünder" die Forderung beeinsprucht hatte, ging die Angelegenheit sofort an ein Inkassounternehmen, mit einer Forderung von € 170.

Als der Konsument für seinen Sohn einen Handyvertrag abschließen wollte, wurde der Vertragsabschluss wegen des negativen Eintrages in einer Bonitätsdatenbank abgelehnt.²

Regine W., seit langem Wertkarten-Kundin bei einem Mobilfunkbetreiber, entschloss sich vor kurzem – übrigens auf Anraten einer dortigen Mitarbeiterin – zu einem Vertragshandy. Sie führte die Anmeldung via Webshop aus, wo sie vom Geburtsdatum über die Passnummer bis zur Kreditkartennummer alle nur möglichen zur Person abgefragten Daten sorgfältig ausfüllte.

Ihre Verblüffung war groß als sie daraufhin nicht freudig als Neu-Kundin begrüßt, sondern lapidar informiert wurde, dass die Mobilfunkfirma einem Vertragsabschluss derzeit nicht zustimmen könne. Ihre gesamte Bestellung sei storniert worden und für nähere Informationen könne sie sich schriftlich an den Mobilfunkbetreiber, zu Handen Credit Check, wenden.

¹ ORF Online 21.05.2008

² ORF Online 17.03.2008

Eine Reaktion, die sich Regine W. nicht erklären konnte. Denn es gibt rein objektiv keinen Grund, an ihrer Bonität zu zweifeln. Sie habe ihr Girokonto noch nie überzogen, habe noch nie einen Kredit aufgenommen, sie sei seit fast zehn Jahren beim selben Arbeitgeber beschäftigt, sei angestellt, beziehe ein regelmäßiges Einkommen, habe keine Gehaltspfändung, die Ablehnung sei für sie daher unverständlich.

Alle Versuche Frau W.'s, den Irrtum über die Einschätzung ihrer Bonität auf kurzem Weg zu klären, scheiterten. Es gab keine Möglichkeit, einen zuständigen Mitarbeiter telefonisch zu kontaktieren und auch nach ihrer schriftlichen Eingabe meldete sich niemand und so fragte Regine W. bei „help“ nach, woher der Mobilfunkbetreiber die falsche Bonitätsauskunft über sie her haben könnte.³

Dies sind nur zwei exemplarisch genannte Fälle wo das Ergebnis einer durchgeführten Bonitätsprüfung im Anschein nach nicht korrekt war und die betroffenen Personen zu Unrecht vom Abschluss eines Handy Vertrages ausgeschlossen wurden. Ist diese Art der Prüfung der Solvenz eines zukünftigen Kunden überhaupt erlaubt ? Was kann nun der/die Betroffene in so einem Fall tun ? Kann er sich gegen Falschinformationen bzw. viel zu alte Informationen wehren ? Welche rechtlichen Möglichkeiten werden ihm vom Gesetzgeber eröffnet ?

³ ORF Online 5.08.2006

2. Zur Entstehung des Datenschutzes

2.1. Die Sphärentheorie

Um die ganze Materie des Datenschutzes besser verstehen zu können, müssen wir uns erst über die Entstehung und die Anfänge besser bewusst werden. Einige Wissenschaftler begründen und definieren den Menschen als ein Individuum welches von verschiedenen Sphären umgeben ist (darum „Sphärentheorie“)⁴ welche durch Einwirkungen von außen verletzt werden können:

- Eigensphäre: Verletzungshandlung: veränderte Wiedergabe von Äußerungen einer Person; heimliche Tonbandaufnahme einer Unterredung soweit dies nicht geschäftsüblich ist
- Geheimsphäre: Verletzungshandlungen: ungenehmigte Veröffentlichung privater Aufzeichnungen; Weitergabe ärztlicher Bescheinigungen – auch nicht peinlichen Inhalts an jemanden – es sei denn, es handelt sich um belanglose Verletzungen und allgemeine Krankheiten; dazu gehört auch die „Intimsphäre“ (lt. BGH definiert als die "innere Gedanken- und Gefühlswelt und den Sexualbereich"). Ein staatlicher Eingriff ist hier ausgeschlossen⁵
- Privatsphäre: dies umfasst das Leben im häuslichen Bereich und Familienkreis sowie das sonstige private Leben. Verletzungshandlungen: zB Veröffentlichung von Auseinandersetzungen innerhalb der Familie; Bekanntgabe von Frauengeschichten; Missachtung der Befugnis des Angehörigen, zu bestimmen, wie das Andenken des Verstorbenen zu bewahren ist⁶

⁴ Hasselkuss/Kaminski in Kilian/Lenk/Steinmüller, Datenschutz, 117; Seidel, Datenbanken und Persönlichkeitsrecht, 65ff

⁵ Im Scheidungsaktenurteil (BVerfG NJW 1969, 1707; BVerfGE 27 wird dieser Bereich absolut geschützt. „Da der Mensch jedoch ein gemeinschaftsbezogenes und – verbundenes Wesen sei, in welchem aber nicht der ganze Bereich des privaten Lebens gehöre. Vielmehr müsse der Bürger in einem nicht absolut geschützten Bereich Eingriffe des Staates hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung der Verhältnismäßigkeit erfolgen. Dort wo an das Verhalten des Menschen in der Außenwelt angeknüpft wird, findet der innerste Bereich sein Grenze“

⁶ K. Wesely, Spannungsverhältnis zw Datenschutz u. betriebswirtschaftlicher Disposition, Dipl.arbeit, Wien 1995

- Individual- oder persönliche Sphäre: die geschäftliche Betätigung im Zusammenhang mit dieser Arbeit als wichtigste Ausformung; sie genießt den relativ schwächsten Schutz. Die Rsp⁷ betont, dass *„der Persönlichkeitsschutz der gewerblichen Betätigung keineswegs soweit reicht wie der Schutz des privaten Bereichs im engeren Sinn. Das Wirken des Menschen im Berufs- und Erwerbsleben vollzieht sich im allgemeinen nicht in einer Geheimsphäre...Es geht nicht an, Grundsätze, die für die Respektierung der sog. Intimsphäre entwickelt wurden, auf den Fall zu übertragen, dass über die Betätigung von Personen im Wirtschaftsleben wahrheitsgemäß berichtet wird...Die Entfaltung der Persönlichkeit im Wirtschaftsleben bringt naturgemäß mit sich, dass sie sich der Kritik stellen muss.“*

Verletzungshandlungen: zB Veröffentlichung eines Bildes ohne Zustimmung des Abgebildeten; Berichterstattung über gewerbliche Tätigkeiten

2.2. Die Mosaiktheorie

Andere wiederum die Informationen nicht in einem so großen Naheverhältnis zur Persönlichkeit stehen sehen, haben die „Sphärentheorie“ erweitert indem sie auch jene Daten in den Schutzbereich einbeziehen möchten, die nicht so persönlichkeitsnah sind, sodass sie nicht zur Privatsphäre eingeordnet werden können. Sie gehen dabei vom dem Gedanken aus, dass aus vielen, an sich ziemlich bedeutungslosen Daten (daher der Name „Mosaiktheorie“)⁸ dennoch ein genaues Persönlichkeitsprofil gebildet werden kann und dadurch das Persönlichkeitsrecht verletzt werden kann. Um dieser Problematik gerecht zu werden, kann man nicht eine exakte Trennungslinie zwischen den Sphären bilden sondern muss erst den Datenaustausch über eine Person in der Gesellschaft untersuchen und danach erst schutzwürdige Bereiche abgrenzen.

2.3. Das rollentheoretische Konzept

Sphären- und Mosaiktheorie versuchen, den Begriff der Privatsphäre durch eine Grenzziehung zwischen „öffentlich“ und „privat“ näher zu erfassen. Dies wird mit dem Versuch des „rollentheoretischen Konzepts“⁹ zu überwinden versucht. Dabei wird auf das

⁷ BGHZ 36, 77 (80); ähnlich LG Dortmund, DB 1966, 1426

⁸ Steinmüller, ADV, 149ff; Seidel, Datenbanken, 66ff

⁹ Steinmüller, ADV, 150; Pawlikowsky, Datenschutz, Leitfaden & Materialien, 18ff

rollenspezifische Verhalten eines jeden Menschen abgestellt. (zB als Ehepartner, Freund, Arbeitnehmer, Steuerzahler, etc). Diese Rolle entspricht einer gewissen Menge an notwendiger Information die für die jeweilige Funktion erforderlich ist. Andere Informationen sind für die jeweilige Rolle nicht erforderlich, unter Umständen sogar störend. Für die Ausfüllung der Rolle kommt es nicht auf das Gesamtbild der Persönlichkeit an, sondern nur auf deren „rollenspezifische“ Züge. Somit bleibt immer ein Rest von Privatheit erhalten, der allerdings entsprechend der sozialen Distanz zum Kommunikationspartner variiert. Die ungleiche Verteilung von Information ist daher durch soziale Rollen bestimmt. Aufbauend auf der Analyse von Kommunikationsstrukturen setzt das „rollentheoretische Konzept“ auf den Grundsatz „*right to share and to withhold*“¹⁰ entgegen die Sphären- und Mosaiktheorie den Grundsatz „*right to be left alone*“ unterstützt.

Egger¹¹ schreibt in diesem Zusammenhang: „*Datenschutz hat im Rahmen dieser Theorie den Zweck, die Zusammenführung der einzelnen Bilder zu verhindern und die Beibehaltung der verschiedenen Bilder zu sichern*“. Dabei werden dem Datenschutz zwei Bedeutungen zugewiesen:

1. Der Schutz der Daten und zwar der Schutz vor Publizität, vor Weitergabe und vor Verknüpfung und
2. der Schutz vor Daten, vor Unvergesslichkeit , vor Objektivitätsverlust und vor Präventivbeschuldigung

¹⁰ Nach Kamlah, Privacy, 97 entspricht dieses Prinzip „zu teilen oder vorzuenthalten“ dem Selbstbestimmungsrecht

¹¹ Egger, Datenschutz versus Informationsfreiheit, 59, 62

2.4. Der Begriff „privacy“

Der amerikanische Begriff „*privacy*“ ist die Grundlage für viele europäische Datenschutzregelungen welche der amerikanische Professor und Politologe *Alan Westin* bereits 1967 wie folgt definiert hat: "*Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about themselves is communicated to others*".

Darin beschreibt er vier Rechte welche integraler Bestandteil der „*privacy*“ sind:

- „*solitude*“ – das Recht, alleine gelassen zu werden
- „*intimacy*“ – das Recht einen Intimbereich zu haben
- „*anonymity*“ – das Recht auf Wunsch anonym bleiben zu können/wollen
- „*reserve*“ – das Recht auf Zurückhaltung/Reserviertheit

Die Sphäre, in der das Recht auf Abgeschiedenheit und Geheimhaltung greift erfuhr in letzter Zeit einen Wandel. Von der Räumlichkeit zu einer *kommunikativ-funktionalen* Auffassung. Entscheidend ist nicht ob sich das Verhalten in den eigenen vier Wänden oder auf der Strasse abspielt, sondern ob in einer konkreten Situation mit der Kenntnisnahme des Verhaltens durch Dritte gerechnet werden musste. Das Recht auf Achtung des Privatlebens sichert dem Bürger daher die Kontrolle über Informationen, die ihn und sein Verhalten betreffen.¹²

Zuerst muss jedoch auch darauf hingewiesen werden, dass der Begriff „*Datenschutz*“ missverständlich sein kann. Geschützt werden nämlich nicht die Daten, sondern natürliche und juristische Personen, deren Daten verarbeitet werden.¹³ Man spricht daher auch von „*personenbezogenen Daten*“ welche § 4 Z 1 DSGVO 2000 als „Angaben über Betroffene deren Identität bestimmt oder bestimmbar ist“ definiert. Personenbezogene Daten sind Einzelangaben

- über „*persönliche*“ Verhältnisse, dh mit der Person verbundene Merkmale (zB Größe, Alter, biometrische Daten)
- und/oder „*sachliche*“ Verhältnisse, dh der Person zuordenbare Merkmale (zB Beruf, Gehalt, Kreditwürdigkeit [Werturteile]¹⁴, Standortdaten bei Mobiltelefonen oder GPS)

¹² Dazu eingehend, *Rüppe*, Der verfassungsrechtliche Schutz der Privatsphäre, 1976, 31ff, 84ff; *Gusy*, Der Schutz der Privatsphäre in der EMRK Art 8 in DuR 13, 1984, 289 (301ff)

¹³ *Hörlsberger*, e-business und Datenschutz, Diss, 65ff

¹⁴ Derartige Informationen brauchen weder wahr oder bewiesen zu sein, um als personenbezogen eingestuft zu werden; vgl hierzu *Duschanek*, § 1 DSGVO 2000 in *Korinek/Holoubek*, Österr BVfR – GR III, Rz 26; derselbe in

- einer bestimmten oder bestimmbaren natürlichen oder juristischen Person.

*Mayer-Schönberger*¹⁵ hat für die Wertungen durch Gesetzgeber und Richter ein bewegliches System mit fünf Elementen zum Schutz der Persönlichkeit postuliert, die verschieden stark ausgeprägt sein können:

- die Nachhaltigkeit und die Verbreitung der Information
- die Bestimmbarkeit des Betroffenen
- die Betroffenheit der Persönlichkeit
- die Marktrelevanz der Information
- die Individualität des Subjekts (welche insb bei juristischen Personen zu prüfen sei)

2.5. Die vier Generationen des Datenschutzes

Es wird auch von den vier Generationen des Datenschutzes gesprochen:¹⁶

Die erste Generation hatte noch die Großrechnertechnologie im Auge und versuchte diese zum Nutzen der Gesellschaft einzusetzen und auch diesbezüglich einzudämmen und mögliche Nachteile abzubauen. Diese begründete Besorgnis und intuitive Angst vor einer alles umfassenden EDV samt Datenbanken, in denen jede Aktivität und Tatsache gespeichert sein würde, entzündete sich exemplarisch an Mitte der sechziger Jahre des vorigen Jahrhunderts in den Industrienationen diskutierten Pläne, die automationsunterstützte Informationsverarbeitung in großem Stil koordiniert einzusetzen. Hier war vor allem das deutsche Bundesland Hessen und Schweden federführend.

In der zweiten Generation der sich neben Österreich auch Frankreich, Spanien, Niederlande, Portugal, Dänemark und Norwegen anschloss, erhielt der einzelne ein Mitspracherecht und die Einwilligung wurde manchmal die Voraussetzung für die Verarbeitung. Die Individualrechte erfuhren eine deutliche Stärkung, sie wurden teilweise grundrechtlich

Duschanek, Der Umfang des Begriffs personenbezogene Daten im DSG in *Duschanek*, Datenschutz in der Wirtschaft (1981), 51 (53); ebenso *Dohr/Pollirer/Weiss*, DSG², § 4 Anm 2

¹⁵ *Mayer-Schönberger*, Information und Recht - Vom Datenschutz bis zum Urheberrecht (2001), 30 mwN

¹⁶ *Brühmann* in *Bäumler/Mutius* (Hrsg), Datenschutzgesetz der dritten Generation, 11ff; *Mayer-Schönberger*, Information und Recht: Vom Datenschutz bis zum Urheberrecht, 113ff

abgesichert und als subjektive Abwehrrechte ausgestaltet.¹⁷ Doch war dies noch ziemlich lückenhaft und unausgegoren und es gab wenig bis keine Regelungen über den internationalen Datenaustausch und wenn dann gingen sie von der Vermutung der Reziprozität aus, ohne entsprechende Garantien zu verlangen. Die Erwartungen und Befürchtungen aus der ersten Generation gingen jedoch in eine ganze andere Richtung als ursprünglich gedacht. Nicht die großen Zentralcomputer mit tausenden Terminals und einer einzigen Datenbank, sondern kleinere Computersysteme begannen den Markt zu dominieren. Aus einer anfangs überblickbaren Anzahl von möglichen Datenschutzverletzer wurde eine fast unüberschaubare Menge von Verwaltungseinheiten und Unternehmen.

In der dritten Generation wurde aufgrund des Volkszählungsurteils des Bundesverfassungsgerichts die Entwicklung des informationellen Selbstbestimmungsrechts in den Vordergrund gestellt. Dies wurde im deutschen BDSG, im österreichischen DSG sowie in Finnland, Norwegen und den Niederlanden insoweit berücksichtigt als die Genehmigungs- und Meldeverfahren zugunsten der Ausdehnung der informationellen Selbstbestimmung des einzelnen verschlankt wurden. Der Gedanke dahinter war sicherlich gut gemeint, doch die technologische Entwicklung und die Dezentralisierung von Datenverwendungen machte es für den einzelnen Betroffenen fast unmöglich über die Verarbeitung seiner personenbezogenen Daten die Übersicht zu behalten. Viele Betroffene scheuten finanzielle Aufwendungen und sonstige Anstrengungen um ihre Rechte geltend zu machen. Die Einwilligung geriet unter kritischer Betrachtung zu einer „gelegten Rutsche“ für die Datenverarbeiter weil den Betroffenen der wirtschaftliche Nutzen nicht immer geläufig war (und auch ist) und er sich mit bescheidenen Vorteilen zufrieden gibt oder als sozial schwächerer Marktteilnehmer auf die gewährten Gegenleistungen angewiesen ist und deshalb keine wirkliche Wahlmöglichkeit besitzt.

In der letzten und vierten Generation versucht der jeweilige nationale Gesetzgeber die Position des einzelnen zu stärken und auch seine Dispositionsfähigkeit (zum eigenen Schutz) einzuschränken. Hier kann auf die Einführung einer verschuldensunabhängigen Gefährdungshaftung und auf die Stärkung der unverzichtbaren Prinzipien der erlaubten Datenverarbeitung, die Unbeschränktheit der Ausübung bestimmter Rechte und auf den ausdrücklichen gesetzlichen Schutz von gewissen persönlichen Daten, verwiesen werden.

¹⁷ Siehe dazu § 1 DSG 1978 sowie Art 35 der Verfassung der Republik Portugal vom 2.4.1976, Art 18 der Verfassung des Königreiches Spanien vom 29.12.1978, Art 10 Verfassung des Königreiches der Niederlande vom 17.2.1983 – alles übersetzt und aus *Kimmel, Die Verfassungen der EG-Mitgliedsstaaten* (1993)

2.6. Datenschutz in der Europäischen Union

Auch im primären Gemeinschaftsrecht der EU wurde dem Datenschutz Rechnung getragen indem in Art 286 EGV die Gemeinschaftsorgane und Einrichtungen einschlägigen Rechtsakten unterworfen wurden.¹⁸

Art 30 Abs 1 lit b EUV ordnet die Beachtung der maßgeblichen Datenschutzvorschriften im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an.

In der „*Charta der Grundrechte der Europäischen Union*“¹⁹ sowie im „*EU-Verfassungsvertrag*“²⁰ wo das Recht auf Datenschutz für die Unionsorgane und deren Einrichtungen sowie die einzelnen Mitgliedsstaaten zur Einhaltung der Europäischen Datenschutzvorschriften verpflichtet wurden, ist die Bedeutung des Datenschutzes innerhalb der europäischen Union festgeschrieben.

Weiters gibt es noch eingehende Datenschutzbestimmungen im Rahmen des Europol-Übereinkommens²¹ und der Schengener Vertragswerke in den Art 102 bis 118 sowie 126 bis 130 des Schengener Durchführungsübereinkommen.²²

Im Bereich des sekundären Gemeinschaftsrecht ist die „*Datenschutz Richtlinie*“ welche auf der Grundlage von Artikel 100a EGV (jetzt Artikel 95 EG) erlassen wurde, die maßgebliche bestimmende Rechtsvorschrift in allen Mitgliedsstaaten. Obwohl die RL 95/46/EG (DS-RL)²³ dies nur für natürliche Personen vorsieht, hat sich der österreichische Gesetzgeber auch für juristische Personen und Personengemeinschaften anwendbar gemacht.²⁴

Dies ergibt sich aus der Definition des „*Betroffenen*“ in § 4 Z 3 DSG 2000 wo darunter jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft zu verstehen ist, deren Daten verwendet werden. Da Verfassungsrecht gemeinschaftsrechtlichen Vorgaben zu folgen hat, ist das Grundrecht im Zweifel richtlinienkonform auszulegen.²⁵ In Deutschland wurde zwar ein schützenswerter Innenbereich für juristische Personen und Personengruppen angenommen, dieser allerdings

¹⁸ Die in Art 286 Abs 2 EGV vorgesehenen Bestimmungen (inkl. eines Europäischen Datenschutzbeauftragten als Kontrollbehörde) wurden mit der Verordnung 2001/45/EG vom 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABI 2001 L 8/1, festgelegt

¹⁹ Teil II, Die Charta der Grundrechte der Union, Art II-68

²⁰ ABI 2004 C 310/I; Teil I, Art I-51

²¹ BGBl III 1998/123; vgl hiezu Weichert, Europol-Konvention und Datenschutz, DuD 1995,450

²² BGBl III 1997/90 idF BGBl III 1997/203

²³ RL des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABI L 281 S 31

²⁴ Juristische Personen unterliegen zwar nicht der DS-RL, aber nach Erwägungsgrund 24 sind einzelstaatliche Rechtsvorschriften zulässig; weiters in Dänemark, Italien und Luxemburg

²⁵ Duschaneck, § 1 DSG in Korinek/Holoubek (Hrsg), Österr BVfR – GR III, Rz 17

als so schwer erfassbar angesehen, dass man befürchtete, damit die Praktikabilität des BDSG zu gefährden und daher wurde davon abgesehen, den Kreis der Betroffenen im BDSG über natürliche Personen hinaus zu erweitern.²⁶

„Ziel der DS-RL ist es, den freien Verkehr personenbezogener Daten innerhalb der Gemeinschaft sicher zu stellen und Wettbewerbsverzerrungen und damit mögliche Risiken einer Standortverlagerung zu beseitigen, indem in allen Mitgliedsstaaten ein gleichwertig hoher Schutz natürlicher Personen bei der Verarbeitung dieser Daten eingerichtet wird.“²⁷

Zentrale Regelungen und Vorgaben der europäischen Datenschutzrichtlinie sind:

- Grundsätzlich keine Unterscheidung zwischen Datenverarbeitung im öffentlichen und nicht öffentlichen Bereich
- Qualität der Daten (Zweckbindungsgrundsatz, Verhältnismäßigkeit, Grundsatz der Richtigkeit und Aktualität)
- Rechtmäßigkeit der Datenverarbeitung (prinzipielles Verbot mit Erlaubnisvorbehalt)
- Festlegung einer Kategorie „sensitiver Daten“ und deren besonderer Schutz
- Privilegierung der Datenverarbeitung für journalistische, literarische und künstlerische Zwecke (Meinungsfreiheit)
- Regelung für eine Datenübermittlung an Drittländer
- Einführung einer Vorabkontrolle
- Pflicht zur Information der betroffenen Person
- Stärkung der Stellung des Datenschutzbeauftragten als „Kontrollstelle“ und der Aufsichtsbehörden; völlige Unabhängigkeit der Kontrollstellen als „ministerialfreier Raum“²⁸

Darunter sind allerdings ausschließlich „*personenbezogene Daten*“ zu verstehen. Dies sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist und diese Daten als geheim halten möchten. Die Datenschutzgruppe hat die Bezogenheit auf eine Person wie folgt definiert: „*Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das*

²⁶ Duschaneck, Datenschutz in der Wirtschaft, 61; Tuner, Datenschutz des Individuums, 721

²⁷ Gemeinsamer Standpunkt des Rates vom 20.2.1995, ABIEG Nr C 93, S 1, 19, Begründung des Rates, II. Ziele

²⁸ Wächter, Datenschutz im Unternehmen (2003), 26; Brühmann in Bäumler/Mutius (Hrsg), Datenschutzgesetz der dritten Generation, 12ff

*Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird.*²⁹

Alternativ dazu kann auch auf das Vorhandensein eines „*Inhaltselements*“ oder eines „*Zweckelements*“ oder eines „*Ergebniselements*“ geprüft werden:

- Ein *Inhaltselement* ist immer dann vorhanden, wenn Informationen über eine bestimmte Person im Zusammenhang mit dem Wort „beziehen“ gegeben werden, unabhängig vom Zweck des für die Verarbeitung Verantwortlichen oder eines Dritten oder von den Auswirkungen auf die betroffene Person.
- Auch ein *Zweckelement* kann dazu führen, dass sich Informationen auf eine bestimmte Person beziehen. Ein solches gilt als gegeben wenn die Daten unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet werden bzw verwendet werden könnten, eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen.
- Von einem *Ergebniselement* spricht man wenn die Verwendung von Daten unter Berücksichtigung aller Begleitumstände auf die Rechte und Interessen einer bestimmten Person Auswirkungen haben.³⁰

Dies wird prinzipiell unmöglich wenn sie allgemein verfügbar sind. „*Allgemein verfügbar*“ ist jedoch nicht unbedingt mit „*veröffentlicht*“ gleichzusetzen.³¹ Die Veröffentlichung von Daten in einem Printmedium oder im Internet für jedermann³² führt dazu, dass diese Daten allgemein verfügbar iSd § 1 Abs 1 letzter Satz DSG 2000 sind und damit kein schutzwürdiges Geheimhaltungsinteresse an diesen Informationen (mehr) besteht.³³

Auch Sachverhaltsdarstellungen fallen darunter wenn die Richtigkeit der Information nachprüfbar ist, also ein objektivierbarer Sachverhalt wiedergegeben wird. Keine Daten sind

²⁹ *Jahnel*, Begriff und Arten von personenbezogenen Daten, Jahrbuch Datenschutzrecht und E-Government, 30

³⁰ *Jahnel*, Begriff und Arten von personenbezogenen Daten, Jahrbuch Datenschutzrecht und E-Government, 31

³¹ vgl. hierzu VwGH vom 14.10.1992, 92/01/0049 wo „Offenkundigkeit“ die jederzeitige Zugänglichkeit der (strittigen) Daten für jedermann voraussetzt wie zB bei Grund- und Firmenbuch. Aber Ergebnisse einer Personensuche im Grundbuch iSd § 360 Abs 3 ASVG sind nicht als „*veröffentlichte Daten*“ anzusehen weil diese Suche nicht jedermann zur Verfügung steht; in den Erl RV 1613 BlgNR XX. GP 35 ist von „*allgemeiner Zugänglichkeit*“ die Rede, ohne auf diesen Begriff näher einzugehen. Er scheint jedoch synonyme Bedeutung zu haben – so auch *Wiederin*, Privatsphäre und Überwachungsstaat, 59; *Dohr/Pollirer/Weiss*, DSG², § 1 Anm 8, 22

³² DSK GZ K120.867/0001-DSK/2004 vom 27. Februar 2004; OLG Innsbruck 27.9.1999 und 28.3.2000, 1 R 143/99k und 1 R 30/00x=MR 2000,148

³³ GZ K120.966/0005-DSK/2005 vom 22. April 2005

daher Einschätzungen oder Urteile. (es kann sich aber allenfalls um Daten der urteilenden Personen handeln !)³⁴

Das Grundrecht auf Geheimhaltung kann jedoch bei Daten, die im Zeitpunkt ihrer Ermittlung allgemein verfügbar waren, wieder aufleben, wenn die allgemeine Verfügbarkeit verloren geht. Eine Datenverarbeitung darf dann nur erfolgen wenn die Voraussetzungen des §§ 6ff DSG 2000 erfüllt sind.³⁵ Andererseits können Daten die ursprünglich als schutzwürdig angesehen worden sind, durch bekannt werden zB im Rahmen eines Prozesses ihre Schutzwürdigkeit verlieren.³⁶ Sie werden dadurch aber nicht als „*allgemein zugänglich*“ iSd § 1 Abs 1 2. Satz DSG 2000 zu qualifizieren sein.

Weiters fallen auch „indirekt“ personenbezogene Daten darunter, die vom Verwender nicht mit rechtlich zulässigen Mitteln auf eine Person zurückgeführt werden können. Aus europarechtlicher Sicht ist dazu anzumerken, dass die DS-RL eine derartige Unterkategorie von personenbezogenen Daten in Art 2 lit a nicht vorsieht. Europarechtliche sind daher indirekt personenbezogene Daten als indirekt identifizierbar und damit als „normale“ personenbezogene Daten zu qualifizieren.³⁷

Öfters ist auch die Meinung anzutreffen, dass Daten die aus öffentlichen Quellen wie zB Telefonbuch, amtliche Verzeichnisse, etc. entnommen werden, ungehindert ermittelt, verarbeitet und auch übermittelt werden dürfen. Das DSG 2000 kennt jedoch keine „freien“ (personenbezogenen) Daten und daher ist die Geltung des DSG unabhängig vom Inhalt und der Herkunft der Daten sobald sie EDV mäßig verarbeitet werden und dadurch selektierbar sind.³⁸ Zu beachten ist jedoch dass auch die Verwendung von Daten abseits jeglicher strukturierter Datei, wie zB ein (Papier-)akt, grundrechtsrelevant sein kann.³⁹

Die Kompetenzgrundlage ergibt sich aus der Verfassungsbestimmung des § 2 DSG 2000 worin – die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsgestützten Datenverkehr Bundessache ist. Die Datenschutz RL verlangt jedoch auch die Einbeziehung von manuell geführten Dateien. Art 3 Abs 1 der Datenschutz RL stellt klar, dass die verwendete Technik für die Sammlung von Daten unabhängig ist weil sonst ernsthafte Risiken der Umgehung bestünden.⁴⁰ Da mit den Ländern keine Einigung

³⁴ So *Duschanek* in *Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben, 295 [299]

³⁵ *Drobesch/Grosinger*, Datenschutzgesetz, Anm 5 zu § 1 Abs 1, 99

³⁶ GZ K120.673/003-DSK/2002 vom 4. Juni 2002

³⁷ So zutreffend *Jahnel*, Begriff und Arten von personenbezogenen Daten, Jahrbuch Datenschutzrecht und E-Government, 36

³⁸ *Wittmann*, Datenschutzrecht im Unternehmen, 13

³⁹ GZ K120.854/0002-DSK/2005 vom 1. Februar 2005

⁴⁰ Erwägungsgrund 27 der DS-RL; *Ghali*, Datenschutz, 240; ebenso *Ehmann-Helfrich*, EG DS-RL (1999) Rz 34 zu Art 2 welche völlig richtig feststellen: „Richtigerweise erkennt der Richtliniengeber, dass die – historisch

diesbezüglich erzielt werden konnte, hat der Gesetzgeber die RL so umgesetzt, dass manuell geführte Dateien für Zwecke von Angelegenheiten, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, nach der einfachgesetzlichen Bestimmung des § 58 DSG 2000 als Datenanwendung nach dem DSG 2000 gelten. Kompetenzrechtlich ist hier neben der Zivilrechtskompetenz insbesondere die Gewerbekompetenz des Bundes von Bedeutung. Daten, die ein Unternehmen zum Betrieb eines Gewerbes manuell erfasst und verwendet, bilden manuell geführte Dateien für Zwecke der Angelegenheiten des Gewerbes.⁴¹ Als weiteres Beispiel sei hier genannt zB manuell geführte Arztkarteien aufgrund des Gesundheitswesens iSd Art 10 Abs 1 Z 12 B-VG wo Gesetzgebung Bundessache ist. Für manuell bearbeitete Dateien welche in die Gesetzgebungskompetenz der Länder fallen, mussten daher in allen neun Bundesländern eigene Landesdatenschutzgesetze erlassen werden. Die hL steht dieser Haltung noch immer äußerst kritisch gegenüber und bemängelt die Übersichtlichkeit und fehlende Bürgernähe aufgrund dieser Kompetenzregelung.⁴²

Gemäß Art 3 Abs 2 der Datenschutz RL finden die Bestimmungen keine Anwendung auf Verarbeitungen für die Ausübung von Tätigkeiten,

- die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen,⁴³ und
- Verarbeitungen personenbezogener Daten durch eine natürliche Person für die Ausübung ausschließlich persönlicher oder familiärer Tätigkeit.

Für den räumlichen Anwendungsbereich nach Erwägungsgrund 19 der EU Datenschutz RL „setzt eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung“ voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich. Zu Erläuterung des Begriffs Niederlassung kann bei der Interpretation des DSG 2000 auf die Definition der Niederlassung in § 4 Z 15 DSG 2000 verwiesen werden. Ausgehend von § 3 DSG 2000 geht das Gesetz vom „Sitzprinzip“ aus. So erhebt zB eine in Frankreich ansässige Konzernmutter Personaldaten von Mitarbeitern eines österreichischen

zu erklärende – Differenzierung nach der Art der Datenverarbeitung ernsthafte Risiken der Umgehung des datenschutzrechtlichen Schutzes eröffnen würde“

⁴¹ Grabenwarter, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 862

⁴² Mayer-Schönberger/Brandl, DSG 2000, (FN 12) 21; Jahnel, Das Datenschutzgesetz 2000, Wichtige Neuerungen, wbl 2000, 49 (55)

⁴³ Somit auch Angelegenheit der Zweiten (Gemeinsame Außen- und Sicherheitspolitik) und Dritten (Zusammenarbeit auf dem Gebiet und Justiz und Inneres) Säule; Ausnahmen sind zB Verarbeitungen betreffend die öffentliche Sicherheit, Landesverteidigung, die Sicherheit des Staates und Tätigkeiten des Staates im Strafrechtsbereich

Tochterunternehmens, gilt für die Zulässigkeit der Datenerhebung französisches (Datenschutz-) Recht. Werden jedoch die Daten bei der Tochterfirma erhoben, so sind die Datenübermittlungen an die Konzernmutter dem österreichischen DSG unterworfen. Ausgangspunkt dieser Regelung ist Art 4 Abs 1 c EU Datenschutz RL, der verhindern soll, dass ein möglicherweise geringer Datenschutzstandard als der in den Mitgliedsstaaten der EU vorhandene in den Fällen zur Geltung kommt, bei welchen Datenerhebungen, -verarbeitungen, -übermittlungen innerhalb der EU durch außerhalb der EU gelegene verantwortliche Stellen vorgenommen werden. Die RL erklärt daher für diese Fälle das „Territorialprinzip“ für anwendbar. Zielsetzung ist damit ein einheitlicher Datenschutzstandard.⁴⁴

§ 3 DSG 2000 drückt auch die in Art 4 Abs 2 EU DS-RL festgelegte Verpflichtung nach Benennung eines Vertreters der für die Datenverarbeitung verantwortlich ist, aus. Die Verpflichtung zur Benennung eines Vertreters will Transparenz in denjenigen Fällen sicherstellen, bei welchen die datenverarbeitende verantwortliche Stelle in einem Drittstaat gelegen ist. Sowohl Betroffene als auch Aufsichtsbehörden sollen einen geeigneten Ansprechpartner haben, dem insoweit Mittlerfunktion zukommt. Das DSG 2000 ist jedoch nicht anwendbar und es sind auch keine Angaben über ansässige Vertreter zu machen, sofern Daten nur zum Zweck der Durchfuhr/Transit eingesetzt werden. (vgl § 3 Abs 3 DSG 2000)

Doch schon der Begriff „Datei“ welcher in der Datenschutz RL in Art 2 lit c und im § 4 Z 6 DSG 2000 wie folgt definiert wurde als „strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind“, schafft Abgrenzungsprobleme welche erst im Laufe der Jahre durch die Rechtssprechung beseitigt wurden. Wie bereits oben erwähnt, gilt dies auch für manuell hergestellte Dateien und dabei ist es unerheblich ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt wurde. Unter „Struktur“ einer Datensammlung wird dabei eine äußere Ordnung – im Gegensatz zum Fließtext – verstanden, nach der die verschiedenen Arten von Daten in einer bestimmten räumlichen Verteilung auf dem oder den manuellen Datenträgern oder in bestimmten physikalischen oder logischen Struktur dargestellt werden. Darüber hinaus müssen die Daten nach bestimmten Kriterien zugänglich sein was in weiterer Folge bedeutet, dass vereinfachte Möglichkeiten des Inhaltszugriffs beispielsweise durch alphabetische und chronologische Sortierung oder durch einen gewissen Automatisierungsgrad, vorliegen

⁴⁴ Siehe auch Wächter, Datenschutz im Unternehmen, (2003) 90f

müssen. Daher sind darunter Karteien und Listen, nicht aber Akten oder Aktenkonvolute zu verstehen.⁴⁵ Auch Klarsichtmappen in die einzelne personenbezogene Dokumente einfach hineingesteckt werden gelten nicht als „Dateien“ und fallen daher nicht unter das DSG.⁴⁶ Ein in einem Zivilprozess erstattetes Sachverständigengutachten ist ohne das erforderliche Suchkriterium keine Datei im Sinne des § 4 Z 6 DSG 2000. (genauso wenig wie ein Zeitungsbericht oder ein Buch wenn nicht das für eine Datensammlung [Datei] charakteristische Spezifikum hinzutritt). Ansonsten müssten auch Akten aus einem behördlichen Verfahren als Datei qualifiziert werden, was eine uferlose Ausweitung des Datenschutzes bedeuten würde.⁴⁷ Obwohl die DS-RL außerhalb automatisierter Verfahren nur die Gewährleistung des Datenschutzes in „Dateien“ verlangt, also in strukturierten Datensammlungen, hätte eine entsprechende Einschränkung des grundrechtlichen Geheimhaltungsanspruches (§ 1 Abs 1 DSG 2000) einen Rückschritt gegenüber dem DSG 1978 bedeutet und wäre somit im Gegensatz zum Grundsatz der Verbesserung des Datenschutzes gestanden. Es besteht daher keine Veranlassung im Geltungsbereich des grundrechtlichen Geheimhaltungsanspruches des DSG 2000, diesen unter Berufung auf die DS-RL einschränkend zu interpretieren.⁴⁸

Eine bloße Erstellung von Texten stellt für sich alleine dann noch keine datenschutzrelevante Datenanwendung dar, wenn die vorhandene Hard- und/oder Software ausschließlich im Sinne einer Schreibmaschine (ohne Archivierungsfunktion) eingesetzt wird. Eine Textverarbeitungssoftware, die vom Auftraggeber zum Zwecke der Informationsarchivierung in der auch Personendaten integriert sind, verwendet wird, fällt unter die Schutzbestimmungen des DSG 2000 genau so wie jedes Textverarbeitungsprogramm wenn dieses über eine Funktion zur Volltextsuche (was bei heutigen Stand der Technik die Regel ist) in erstellten oder archivierten Textdokumenten verfügt. Stellt eine Textverarbeitung einen Teil einer umfassenden Datenanwendung zB durch ein Aktenverwaltungssystem dar, so teilt die Textverarbeitung das datenschutzrechtliche Schicksal dieser umfassenden Datenanwendung.⁴⁹

⁴⁵ So auch *Mayer-Schönberger/Brandl*, DSG 2000, 62ff

⁴⁶ *Dammann-Simitis*, EG DS-RL, 88

⁴⁷ OGH 6 Ob148/00h vom 28. Juni 2000; aA die DSK hat in stRsp jedoch allen Daten welche auch nicht in einer Datei vorhanden sind, das Recht auf Geheimhaltung zugesprochen

⁴⁸ *Rosenmayr-Klemen*, Zum Schutz manuell verarbeiteter Daten durch das DSG 2000, *ecolex* 2001, 641 mit Kritik an OGH 28.6.2000, 6 Ob 148/00h = SZ 73/105; ebenso VwGH 21.10.2004, 2004/06/0086/ und *Dohr/Pollirer/Weiss*, § 4 Anm 7

⁴⁹ *Trotzmüller*, Die Durchsetzbarkeit des Rechts auf Datenschutz im Lichte der Judikatur, Diss Uni Wien, 70ff

Datenschutz setze das Vorliegen einer entsprechend strukturierten Datei voraus. Diese Entscheidung wurde von *Rosenmayr-Klemen*⁵⁰ dahin kritisiert, dass der Oberste Gerichtshof nicht zwischen der Geheimhaltung gemäß § 1 Abs 1 DSG 2000 und dem Recht auf Auskunft, Richtigstellung und Löschung gemäß § 1 Abs 3 DSG 2000 differenziere. Damit bleibe ungeachtet, dass § 1 Abs 1 DSG 2000 allgemein von "Daten", Abs 3 jedoch von Daten, die zur Verarbeitung in manuell geführten "Dateien" bestimmt sind, spreche. In diesem Sinn ist wohl auch die Kommentierung von *Drobesch/Grosinger* zu verstehen, nach der das Grundrecht auf Geheimhaltung alle personenbezogenen Daten unabhängig davon erfasse, ob sie in einer Datei (vgl § 4 Z 6 DG 2000) strukturiert gesammelt werden oder nicht.⁵¹ Auch das bloße Wissen ohne Aufzeichnung kann unter den Begriff der personenbezogenen Daten fallen und ist sodann grundsätzlich dem Datenschutz unterworfen. Allerdings unterliegt derartiges persönliches Wissen ebenso wie unstrukturiert aufgezeichnete Angaben „nur“ dem Grundrecht auf Geheimhaltung nach § 1 Abs 1 DSG 2000.

Das Grundrecht als höchstpersönliches Recht steht nur lebenden Personen zu. Zu beachten ist aber, dass Daten Verstorbener sich zeitgleich auf andere lebende Personen beziehen können und daher wieder schützenswert sind.

Die Umsetzung der DS-RL brachte auch eine Erweiterung der Kontrollfunktionen der DSK als unabhängige Kontrollstelle mit umfassender Zuständigkeit iSd

Art 28 DS-RL und ist im Verfassungsrang verankert.(§§ 35 Abs 2, 37 Abs 1 und 2, 38 Abs 1)⁵²

Durch die Regelungen in der Datenschutz RL 95/46/EG wird zwar der Vorrang des freien Datenverkehrs im Binnenmarkt zugunsten nationaler Datenschutzregelungen manifestiert⁵³ jedoch auch andererseits wird durch die Bestimmungen in Art 1 Abs 1 der DS-RL das Grundrecht auf Schutz der Privatsphäre im Sinne des Art 8 EMRK ebenso wie weiterer Grundrechte konkretisiert⁵⁴.

⁵⁰ *Rosenmayr-Klemen*, Zum Schutz manuell verarbeiteter Daten durch das DSG 2000, *ecolex* 2001, 639

⁵¹ OGH 10b109/02i vom 25. Juni 2002

⁵² *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), *Österr BVfR-GR III*,

⁵³ Art 1 Abs 2 DS-RL lautet: „ Die Mitgliedstaaten beschränken oder untersagen nicht den freien Datenverkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Abs 1 gewährleisteten Schutzes“.

⁵⁴ Art 1 Abs 1 DS-RL lautet:“ Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“. Neben dem Grundrecht auf Datenschutz weisen auch andere Grundrechte, wie zB das Brief- und Fernmeldegeheimnis, das Hausrecht, die Meinungsäußerungsfreiheit datenschutzrechtliche Bezüge auf (vgl *Duschanek*, Neuerungen und offene Fragen im DSG 2000; *Dammann/Simitis*, EG DS-RL, Kommentar (1997), 101

2.7. Datenschutz in Österreich

2.7.1. Die Entstehung des Datenschutzes in Österreich

- 1971 wurde in Österreich mit der Einrichtung einer Arbeitsgruppe „Datenschutz“ im Rahmen des Koordinationskomitees für die elektronische Datenverarbeitung im Bereich des Bundes unter dem Vorsitz des Verfassungsdienstes des BKA begonnen.
- Am 20. Februar 1973 kam es zu einem Vorentwurf für ein DSG aufgrund der Ergebnisse der Arbeitsgruppe
- Am 1. August 1973 gab es einen (zweiten) Referentenentwurf des DSG welcher sich nur auf Dateien von Einrichtungen des Bundes bezog und keine Verfassungsbestimmung vorsah
- Am 16. Mai 1974 kam es zu einem (revidierten) Entwurf des Bundesdatenschutzgesetzes (GZ 51.500-2d/74)
- Am 18. Dezember 1974 folgte die 1. RV eines DSG; neu eingebracht am 16. Dezember 1975
- Ebenfalls 1975 fasste das Europäische Parlament entsprechende Entschlüsse⁵⁵, aber erst 1990 wurden Regelungsvorschläge von der Kommission vorgelegt⁵⁶.
- Am 18. Oktober 1978 kam es zur Verabschiedung des DSG 1978 im Nationalrat
- 1. Jänner 1980 In Kraft treten des DSG 1978 in Österreich
- Zwischen 1981 und 1989 wurde das Gesetz sechsmal novelliert
- 15. Februar 1999 Einlangen der RV 1614 zum DSG 2000
- 13. Juli 1999 Abänderungsanträge; Zweite + Dritte Lesung im NR; Annahme
- 1. Jänner 2000 In Kraft treten des DSG 2000 (BGBl. I Nr. 165/1999)
- 2001, 2005 und 2008 erfolgte jeweils eine Novellierung des DSG 2000

Der Begriff des Datenschutzes hat sich in Österreich und Deutschland Anfang der 80er Jahre des vorigen Jahrhunderts gebildet.⁵⁷ 1984 sah das deutsche BVerfG in der Entscheidung „Volkszählungsurteil“ den Begriff in Art 2 Abs 1 GG⁵⁸ verankert und machte so den

⁵⁵ Entschlüsse vom 13.3.75, ABIEG C 60, 48; ABIEG C 100, 27; ABIEG C 140, 34.

⁵⁶ ABIEG 1990 C 277, 3

⁵⁷ Grundlegend Stadler, Das österreichische Datenschutzgesetz als Markstein der Verfassungspolitik und des Informationsrechts, JBl 1979, 358ff

⁵⁸ Art 2 Abs 1 GG lautet „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“.

partizipativen Datenschutz in Deutschland zum Grundrecht.⁵⁹ Mit dieser Ansicht hat Deutschland in Europa eine Vorreiterrolle übernommen welche sich mittlerweile europaweit durchgesetzt hat auch wenn das informationelle Selbstbestimmungsrecht nirgends ausdrücklich positiviert ist.⁶⁰

*Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. [...] Dieses Recht auf „informationelle Selbstbestimmung“ ist nicht schrankenlos gewährleistet [...] Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung hinnehmen. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.*⁶¹

Die informelle Selbstbestimmung⁶² ist die Befugnis des einzelnen grundsätzlich frei und selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.⁶³ Das informelle Selbstbestimmungsrecht besteht aus zwei Komponenten:

1. Geheimnisschutz: Der Betroffene bestimmt, wer, was, wann über ihn erfährt. Er kann Daten geheim halten. Personen geben keine Informationen über den/die Betroffenen ohne dessen Wissen und Einverständnis weiter
2. Informationsrecht: Der Betroffene kann sich über den Wissensstand anderer Personen über ihn informieren. Unsicherheiten in der Kommunikation werden damit verringert

⁵⁹ Dammann, NJW 1984, 398 ff nennt es jedoch „nicht die Geburtsstunde eines neuen Grundrechts“ und insbesondere nicht „eines Grundrechts auf Datenschutz“ sondern nur die Fortbildung der differenzierten Rechtssprechung des BVerfG zum allgemeinen Persönlichkeitsrecht; ebenso Denninger in Hohmann (Hrsg), Freiheitssicherung durch Datenschutz, 127 ff

⁶⁰ Mayer-Schönberger/Zeger/Kronegger, Auf dem Weg nach Europa: Zur Novellierung des DSG, ÖJZ 1998, 246

⁶¹ U 15.12.1983, BVerfGE 65,1f – Volkszählungsurteil = 1BvR 209/83, hier 45+46 = NJW 1984, 419ff; dazu auch Mayer-Schönberger/Brandl, DSG 2000, 13f

⁶² Dieser Rechtsanspruch steht jedoch zwangsläufig in Konflikt mit Art 13 StGG und Art 10 EMRK, so Berka, Grundrechte, Rz 550f, 571

⁶³ VfGH 14.3.1991, VfSlg 12.689/1991, 510 der dazu ausführt, „es sei das Recht des Betroffenen, in der Führung seines Lebens und seiner Sozialkontakte selbst zu entscheiden, ob und wa er darüber welchen anderen wissen lässt.“

⁶⁴ Weitenbacher, Datenschutz in Banken im Hinblick auf einen Beitritt Österreichs zur EU, Dipl.arbeit (1993)

Mit diesem Recht wandelt sich der Datenschutz von einem klassischen Abwehrrecht zu einem Gestaltungsauftrag, der den Gesetzgeber verpflichtet, dem Bürger Einflussmöglichkeiten auf die ihn betreffenden Datenströme einzuräumen. Ist dem Bürger dieser Einfluss entzogen, weil ihm Daten abverlangt werden oder weil Daten ohne seine Zustimmung übermittelt werden dürfen, so bedarf es dafür gesetzlicher Regelungen mit ausreichender Bestimmtheit, Klarheit und Nachvollziehbarkeit.⁶⁵ Der Betroffene kann als Ausfluss dieses „*informationellen Selbstbestimmungsrechts*“ jederzeit die Zustimmung zur Datenverwendung widerrufen (§ 1 Abs 2 iVm 8 Abs 2 Z 2 DSG 2000). Das Recht auf Geheimhaltung personenbezogener Daten ist zwar ein absolutes Recht, aber in seinem Anwendungsbereich nicht absolut, sondern einer Interessensabwägung unterworfen. Es besteht nur, soweit der Betroffene daran ein schutzwürdiges Interesse, insbesondere in Hinblick auf die Achtung seines Privat- und Familienlebens, hat. Durch ein zweistufiges Prüfungsverfahren ist zuerst die Schutzwürdigkeit des Interesses des Betroffenen zu prüfen und sodann gegen das Interesse anderer auf Informationszugang abzuwägen. Dieses Interesse muss gesetzlich normiert sein oder sich auf andere Grundrechte beziehen und überdies die engen Voraussetzungen des Art 8 Abs 2 EMRK erfüllen. (§ 1 Abs 2 DSG 2000) Stehen einander zwei gleichrangige grundrechtliche bewehrte Interessen gegenüber, wiegen im Zweifel die Interessen des Betroffenen mehr.⁶⁶

Eine Besonderheit des österreichischen Datenschutzrechts im internationalen Vergleich besteht darin, dass in Österreich nicht nur Daten von natürlichen Personen, sondern auch (noch !) Daten von juristischen Personen⁶⁷ und Personengemeinschaften wie etwas handelsrechtliche Personengesellschaften, GesnBR oder Hauseigentümergeinschaften geschützt werden. Dies betrifft vor allem Geschäftsgeheimnisse worunter man Produktionsverfahren, Kostenstruktur, Patente, Kundendaten, Organisationsmaßnahmen und Mitarbeiterdaten versteht. Der Grundrechtsschutz wird in Österreich juristischen Personen auch sonst zuerkannt, soweit das jeweilige Grundrecht seinem Wesen nach dafür geeignet ist.⁶⁸

⁶⁵ *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006), 329

⁶⁶ *Mayer-Schönberger*, Information und Recht: Vom Datenschutz bis zum Urheberrecht, 46 mwN und 144

⁶⁷ Für Deutschland, BGH vom 17.12.1985, NJW 1986, 2505 ff (=CR 1986, 635ff) der auch Angaben über die finanzielle Situation einer GmbH als personenbezogene Daten ansieht obwohl nicht im BDSG erwähnt; weiteres keinen Schutz für juristische Personen bietet zB das dänische, französische, finnische, schwedische und britische DSG

⁶⁸ VfSlg 2088/1951, 3495/1959, 5531/1967

2.7.2. Das Grundrecht auf Datenschutz⁶⁹

Entgegen der Vermutung der Bestimmung des § 1 DSG 2000 gibt es kein einheitliches Grundrecht auf Datenschutz. Es besteht aus mehreren, unterschiedlichen Rechten:⁷⁰

- Das Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000)⁷¹
- das Recht auf Auskunft (§ 1 Abs 3 Z 1 DSG 2000)
- das Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 DSG 2000)
- das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs 3 Z 2 2. Satz DSG 2000)

Das Zusammenwirken dieser Ansprüche und der zu ihrer Ausführung ergangenen einfachgesetzlichen Vorschriften darf das vom deutschen BVerfG entwickelte Modell der „*informationellen Selbstbestimmung*“ auch in der österreichischen Rechtsordnung als verwirklicht angesehen werden.⁷² Das Grundrecht auf Datenschutz iSd § 1 DSG 2000 gewährleistet einen umfassenden Schutz personenbezogener Daten.⁷³ Voraussetzung dafür ist jedoch die Schutzwürdigkeit der fraglichen Information, sodass die Reichweite des Schutzes von einer abwägenden Beurteilung der Schutzwürdigkeit abhängt.⁷⁴ Ob solche ein schutzwürdiges Geheimhaltungsinteresse vorliegt, ist nach § 1 Abs 1 DSG 200 gesondert zu prüfen.⁷⁵ Als Richtschnur gilt die hL und Rspr zu § 1 DSG 1978 denen zufolge die Schutzwürdigkeit nach den Wertungen der gesamten Rechtsordnung zu bestimmen ist.⁷⁶

Dieses nationale Grundrecht wird im Geltungsbereich des EU-Rechts durch das europäische Grundrecht auf Datenschutz ergänzt, welches jedoch ein ungeschriebenes Grundrecht ist, aber durch Art 8 der Europäischen Grundrechte-Charta⁷⁷ in Anlehnung an die DS-RL sichtbar

⁶⁹ Ausführlich hiezu *Wiederin*, Privatsphäre und Überwachungsstaat (2003), 57ff sowie *Duschanek* in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, § 1 DSG 2000

⁷⁰ In VfSlg 12.194/1989 wird klargestellt, dass das Grundrecht auf Datenschutz nicht auf den Geheimhaltungsanspruch beschränkt ist, sondern auch die Ansprüche auf Auskunft, Richtigstellung und Löschung umfasst

⁷¹ Der VfGH schliesst auch die *Datenermittlung* darunter ein; VfSlg 12.228/1989, 12.880/1991, 16.369/2001

⁷² So *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR-GR III, Rz 16; zB hinsichtlich des Ausschlusses der Geheimhaltung mangels schutzwürdiger Interessen (§ 1 Abs 1 2. Satz), Beschränkungen der Geheimhaltung (§ 1 Abs 1 1. Satz), Verwendung besonders schutzwürdiger Daten (§ 1 Abs 2 2. Satz)

⁷³ Vgl hiezu *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR-GR III

⁷⁴ So *Dohr/Pollirer/Weiss*, DSG², § 1 Rz 7; *Wiederin*, Privatsphäre und Überwachungsstaat, 60ff; aA *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR-GR III, Rz 42

⁷⁵ So auch *Dohr/Pollirer/Weiss*, Datenschutzrecht § 1 DSG Anm 7; *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR-GR III, Rz 40ff

⁷⁶ *Jahnel*, Datenschutzrecht, 250ff

⁷⁷ Artikel 8 - Schutz personenbezogener Daten

(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

gemacht wurde.⁷⁸ Diese Grundrechte sind wiederum mit dem Recht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK systematisch verknüpft wobei insbesondere der Geheimnis- und Datenschutz mit umfasst wird.⁷⁹ Auch der Entwurf des Konvents für einen EU-Verfassungsvertrag beinhaltet das Recht auf Datenschutz und verpflichtet die Unionsorgane und Einrichtungen sowie die Mitgliedsstaaten zur Einhaltung der Europäischen Datenschutzvorschriften.⁸⁰

Mit dem Grundrecht auf Datenschutz wurde in Entsprechung des Art 8 Abs 1 der Europäischen Menschenrechtskonvention (EMRK) das Recht auf Schutz der Privatsphäre weiter ausgebaut. Auch der EGMR anerkennt in seiner Rechtssprechung ausdrücklich, dass das Sammeln, Speichern und Bearbeiten von Daten sowie deren Verwendung und Weitergabe einen Eingriff in das Recht auf Achtung des Privatlebens darstellen könne.

Der Datenschutz ist dabei ein Anspruch des Einzelnen auf Geheimhaltung personenbezogener Daten, dies auch bei bloß manueller Datenverarbeitung, etwa mittels einer Kartei (das Vorliegen einer „Datei“ ist nicht erforderlich), soweit der Betroffene daran ein schutzwürdiges Interesse, insbesondere in Hinblick auf Achtung seines Privat- und Familienlebens, hat. Der Text des § 1 DSG 2000 macht deutlich, dass der Schutzzweck über die Achtung des Privat- und Familienlebens hinausgeht und auch den Bereich des wirtschaftlichen oder politischen Lebens mit einschließt.⁸¹ Schutzwürdig sind daher insb Angelegenheiten der Privatsphäre eines Menschen, Geschäfts- und Betriebsgeheimnisse sowie Daten, die dem Steuer- oder Bankgeheimnis unterliegen oder einem Parteienvertreter überlassen wurden.⁸² Weiters zählen hiezu Zahlungs-, Nachfrage- oder Freizeitverhalten, rechtliche oder sonstige Beziehungen, Einkommen⁸³ und Vermögen, Einstellungen, Aktivitäten usw. Auch *Werturteile*⁸⁴ wie zB Charaktereigenschaften, medizinische Diagnosen, Kreditwürdigkeit, Arbeitseinstellung fallen darunter ebenso personenbezogene Planungen und Prognosen weil sie Angaben über Betroffene iS der gesetzlichen Definition liefern. Um dies extra zu betonen und zu

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.

⁷⁸ *Mähring*, Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht, EuR 1991, 369; *Siemen*, Datenschutz als europäisches Grundrecht (2006)

⁷⁹ *Wiederin*, Art 8 EMRK in *Korinek/Holoubek* (Hrsg), Österr BfVR – GR III, Rz 51

⁸⁰ ABI 2004 C 310/I; Teil I, Art I-51

⁸¹ *Dohr/Pollirer/Weiss*, Datenschutzrecht § 1 DSG, Anm 5; *Jahnel*, Datenschutzrecht, 251; VfGH 28.11.2001, B 2271/00; OGH 29.3.200, 6 Ob 77/00; 28.6.2000, 6 Ob 162/00t = EvBl 2001/3; 28.6.2000, 6 Ob 163/00i = EvBl 2001/4; ebenso zuvor zum DSG 1978 12.228/1989, 12.880/1991; OGH 15.12.1999, 6 Ob 307/99m = RdW VfSlg 2000/250, 283; *Duschaneck*, FS Rill 421 mwN; *Feik*, Datenschutzrechtliche Überlegungen zum Umweltinformationsgesetz (UIG), ÖJZ 1995, 13 (15ff)

⁸² *Jahnel*, Datenschutzrecht, 250ff

⁸³ EuGH, Rechnungshof, Slg 2003, I-04989, Rz 64; VfSlg 17.065/2003; OGH 21.1.2004, 9 Ob A 77/03v

⁸⁴ Vgl *Dohr/Pollirer/Weiss*, § 4 Anm 2; *Dammann/Simits*, § 3 BDSG, Rz 12

verdeutlichen, hat der Verfassungsgesetzgeber den Hinweis auf die Achtung des Privat- und Familienlebens im Vergleich zu § 1 Abs 1 DSG 1978, in den ersten Satzteil des § 1 Abs 1 DSG 2000 (vor-) gezogen.⁸⁵

Der OGH hat jedoch bei unterhaltsrechtlichen Streitigkeiten die Schutzwürdigkeit von Informationen betreffend die Wirtschaftssphäre eines Menschen anders eingestuft.⁸⁶ Dieses Grundrecht steht „jedermann“⁸⁷ zu, es handelt sich daher um ein Menschen- und angeborenes Recht iSd § 16 ABGB⁸⁸, geschützt sind allerdings auch juristische Personen wie eine GesmbH oder ein Verein sowie Personengemeinschaften wie eine Bürgerinitiative, sofern das Grundrecht auf Datenschutz als das subjektive Recht des Einzelnen auf Geheimhaltung begrifflich für diesen Kreis zur Anwendung kommen kann.⁸⁹ Selbst das Zusammentragen personenbezogener Informationen aus offenen Quellen und die Verwendung und die die Verwendung freiwillig preisgegebener Daten kann Art 8 EMRK berühren wenn es sodann zB zu einer Verdichtung in Persönlichkeitsprofilen oder zu einer Zweckentfremdung kommt.⁹⁰ Als weitere Verfassungsbestimmungen gilt die Einrichtung der Datenschutzkommission (DSK) als weisungsfreies Kontrollorgan in Form einer Kollegialbehörde gem Art 20 Abs 2 B-VG.⁹¹

Das Schutzgut des Grundrechts auf Geheimhaltung umfasst zunächst den Geheimhaltungsschutz im engeren Sinn, also einen Schutz vor Übermittlung und Preisgabe von Daten. Daneben ist das Grundrecht nach einhelliger Meinung⁹² aber auch gegen die zwangsweise Verpflichtung des Betroffenen oder eines Dritten zur Weitergabe oder Offenlegung der Daten gerichtet und schützt somit auch vor Versuchen, die Daten auf andere Weise (etwa durch Täuschung) in Erfahrung zu bringen und bewirkt dadurch auch einen Ermittlungsschutz. Auch „Ersatzvornahmen“ wie die Befragung Dritter oder die heimliche Erhebung der gewünschten Informationen beim Betroffenen sind als indirekte

⁸⁵ Kotschy, Grundrecht, 89 (FN 1)

⁸⁶ OGH SZ 2004/39

⁸⁷ Einige Grundrechte in der österreichischen Rechtsordnung sind jedoch an die österreichische Staatsbürgerschaft gebunden wie zB der Gleichheitsgrundsatz (Art 7 B-VG und Art 2 StGG); hiezu auch Jahnelt, Das Grundrecht auf Datenschutz in FS Schäffer, 315

⁸⁸ § 16 ABGB lautet: *Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten.* Juristische Personen können sich daher nicht auf § 16 ABGB berufen auch wenn ihnen manche Rechte wie zB Namen, Ehre zustehen.

⁸⁹ VfSlg 2088/1951, 3495/1959, 5531/1967

⁹⁰ EGMR, Fall *Rotaru*, Z 43 f, zu einer systematischen Sammlung und behördlichen Speicherung von Daten, welche die weit zurückliegende Vergangenheit betrafen

⁹¹ §§ 35 DSG 2000

⁹² Rill, Grundrecht auf Datenschutz, 26; ihm folgend VfSlg 12.228/1989, 12.880/1991 und 16.369/2001; Drobesh/Grosinger, DSG, Anm 3 zu § 1 Abs 1 98; stRsp der DSK zB GZ K121.009/0010 vom 21. Juni 2005

Informationseingriffe am Grundrecht zu messen.⁹³ § 1 Abs 1 DSG 2000 schützt daher auch Daten, die nicht in einer Datenanwendung gespeichert sind, also auch Daten, die lediglich mündlich weitergereicht und nicht archiviert werden.⁹⁴ Dies ergibt sich aus dem Wortlaut und einem systematischen Vergleich von § 1 Abs 1 mit Abs 3 DSG 2000.

In bestimmten Bereichen (zB bei Mitteilungen im Rahmen sozialüblicher privater Kommunikation über Lebensumstände anderer) wird dies jedoch teleologisch zu reduzieren sein. Aufgrund des Hinweises auf den Schutz des Privat- und Familienlebens in § 1 Abs 1 DSG 2000, geht das Grundrecht auf Datenschutz über diesen Rahmen hinaus und reicht bis in den Bereich des wirtschaftlichen und politischen Lebens.⁹⁵

Auch durch die Vernichtung von Datenträgern um das Geheimhaltungsgebot zu umgehen, kann die Bindewirkung des Grundrechts nicht aufgehoben werden.⁹⁶

Nach bisher einhelliger Judikatur und Literatur handelt es sich um ein höchstpersönliches Recht, das mit dem Tod des Betroffenen erlischt und nicht auf Rechtsnachfolger übergeht. Wenn man daher von Daten iSd DSG 2000 spricht, sind immer Daten von lebenden Personen gemeint weil nur sie Träger des Grundrechts auf Datenschutz in Frage kommen. Als Persönlichkeitsrecht kann es jedoch grundsätzlich über den Tod des Betroffenen hinauswirken.⁹⁷ Es kann daher nicht wie ein dingliches Recht übertragen oder vererbt werden. Lediglich kann anderen der Eingriff in das Recht gestattet werden. Diese Gestattung ist jedoch kein Rechtsverzicht, sondern eine Ausübung des allgemeinen informationellen Verfügungs- und Gestaltungsrechts.⁹⁸

Schließlich kommt dieses Grundrecht zwischen Privaten *unmittelbar* zur Anwendung (*Drittwirkung* gem. § 1 Abs 5 DSG 2000)⁹⁹ und wirkt über § 16 ABGB mittelbar in das

⁹³ *Wiederin*, Privatsphäre und Überwachungsstaat, 62; auch der aus § 16 ABGB abgeleitete Geheimhaltungsanspruch betreffend Fakten der Privatsphäre wird so versandt, dazu *Koziol*, Österreichisches Haftpflichtrecht II, 14 mwN

⁹⁴ Vgl ebenso *Dohr/Pollirer/Weiss*, DSG², § 1 Anm 6; OGH in JBl 1997, 516; *Schobel*, Verletzung von Geheimhaltungspflichten durch Banken, ÖBA 2004, 8

⁹⁵ *Dohr/Pollirer/Weiss*, DSG², § 1 Anm 5, 20; bei der Abgrenzung von staatlichen Überwachungsmaßnahmen siehe *Wiederin*, Privatsphäre und Überwachungsstaat, 62ff

⁹⁶ Auf persönliches Wissen gestützte Mitteilungen fallen nicht darunter; *Rill* in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, 18ff

⁹⁷ *Drobesch/Grosinger*, DSG, Anm 3 zu § 1 Abs 1, 98; GZ K202.028/006-DSK/2003 vom 12. September 2003

⁹⁸ *Geiger*, Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1989, 36

⁹⁹ Vgl *Berka*, Lehrbuch Grundrechte (2000), Rz 281; *Grabenwarter*, Informationsgesellschaft 63; *Walter/Mayer*, Bundesverfassungsrecht, Rz 1492; *Dohr/Pollirer/Weiss*, Datenschutzrecht², § 1 DSG Anm 2; *Drobesch/Grosinger*, Das neue österreichische DSG (2000), 98; *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BfVR – GR III, Rz 18; aA *Öhlinger*, Verfassungsrecht Rz 742, der unmittelbare Drittwirkung für unmöglich hält sowie *Stocker*, Datenschutz im öffentlichen Bereich, Diss Salzburg 2002, 118f, der die Drittwirkung nur dem Geheimhaltungsanspruch zuerkennt und die Begleitansprüche Auskunft, Richtigstellung und Löschung auf eine Konkretisierung und Ausgestaltung durch den Gesetzgeber annimmt.

Zivilrecht.¹⁰⁰ Die *Drittwirkung* beschränkt sich jedoch nicht nur auf den Geheimhaltungsanspruch, sondern erstreckt sich auch auf die unberechtigte Ermittlung und Weitergabe von zulässig oder unzulässig ermittelten Daten sondern auch auf Leistungsansprüche wie Auskunft, Richtigstellung und Löschung. Die Verfassungsbestimmung des § 1 DSG 2000 kann durch den Verweis auf die Achtung des Privat- und Familienlebens im Sinne der EMRK auch als eine Art „*lex specialis*“ zu dieser gesehen werden, da Eingriffe nur in den in Abs 2 genannten Voraussetzungen zulässig sind. Der Eingriff darf nur mit der gelindesten, zum Ziel führenden Art und Weise durchgeführt werden. Dies bedeutet in der Praxis, dass verfassungsrechtlich geschützte Rechte nicht durch „einfache“ Gesetze unterlaufen werden können und schutzwürdige Interessen dann einfach nicht (mehr) bestehen sollen.¹⁰¹ Der VfGH hat für die Verletzung von Grundrechten folgende Formel entwickelt: *„Das Grundrecht ist verletzt, wenn der Verwaltungsakt unter Heranziehung eines verfassungswidrigen Gesetzes oder ohne gesetzliche Grundlage, also gesetzlos, ergangen ist, wobei der Gesetzlosigkeit die nur scheinbare und die so genannte denkunmögliche Gesetzesanwendung gleichzuhalten ist.“*¹⁰²

Die Formulierung „derartige Gesetze“ in § 1 Abs 2 2. Satz DSG 2000 im Zusammenhang mit den Erläuterungen ergibt, dass dem Gesetzgeber aufgetragen wird, Eingriffe nur aufgrund von Gesetzen im formellen Sinn zu erlauben, nicht aber aufgrund von Rechtsverordnungen.¹⁰³

Bei den nach § 1 Abs 3 DSG 2000 verfassungsgesetzlich gewährleisteten Rechten betreffend der Auskunft, wer Daten verarbeitet, woher diese stammen und wozu sie verwendet und an wen sie übermittelt werden sowie die Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteten Daten haben im Unterschied zum Geheimhaltungsrecht nach § 1 Abs 1 DSG 2000 zur Voraussetzung, dass die betreffenden Daten zur automationsunterstützten oder zur manuellen Verarbeitung in Dateien bestimmt sind. (näheres siehe unten Kapitel 14.)

¹⁰⁰ Weiss/Pollirer, Datenschutz in der Wirtschaft, RWZ 1993/4, 115; Dohr/Pollirer/Weiss, DSG², § 1 Anm 29, 25; Drobesh/Grosinger, DSG, Anm 1 zu § 1 Abs 5, 102; Janel in FS Schäffer, 337 mwN; Posch in Schwimann², Rz 42 zu § 16

¹⁰¹ Kunnert, Section Control, ZVR 2006/17

¹⁰² VfSlg 5463/1967, 7856/1976, 8472/1978; wobei unter „Gesetz“ eine Rechtsvorschrift von unterverfassungsgesetzlichen Rang verstanden wird

¹⁰³ Erl RV 1613 BlgNR 20.XX GP 35; Dohr/Pollirer/Weiss, DSG², § 1 Anm 16, 24; Andernfalls könnte eine Verwaltungsbehörde sich selbst mittels Verordnung die Befugnis für ihren eigenen Eingriff in das Grundrecht auf Datenschutz schaffen

Bei juristischen Personen kommen diesbezüglich nach hL und stRsp Wirtschaftsdaten sowie Daten aus dem Kunden- und Lieferantenverkehr¹⁰⁴ oder Geschäfts- und Betriebsgeheimnisse¹⁰⁵ in Betracht. Der OGH sieht jedoch auch die Offenlegungspflicht bei Kapitalgesellschaften (siehe hiezu unten Kapitel 3.3.) in Bezug auf den Gläubigerschutz als gerechtfertigt an.¹⁰⁶

Nach der Rechtsprechung des VfGH genießen Informationen die einem Arzt oder Rechtsanwalt anvertraut wurden, höhere Schutzwürdigkeit als jene die einem Ziviltechniker anvertraut wurden.¹⁰⁷

Wird jedoch ein Interesse von der Rechtsordnung im vornhinein nicht als schutzwürdig anerkannt, so ist die Abwägung mit anderen, kollidierenden Interessen nicht erforderlich. Eine Interessensabwägung ist daher bei der Feststellung des Schutzbereichs des Grundrecht noch nicht durchzuführen sondern erst im Rahmen des § 1 Abs 2 DSG 2000 bei der Prüfung der Rechtfertigung des Eingriffs, wenn zuvor das Bestehen eines schutzwürdigen Interesses bejaht worden ist.¹⁰⁸

Die Informationskontrolle über das Recht des einzelnen auf Achtung seines Privatlebens bewirkt, dass die Entscheidung darüber Informationen über sich geheim zu halten oder preiszugeben beim jeweiligen Betroffenen liegt. Niemand muss/soll dazu angehalten werden bzw. muss damit rechnen, dass personenbezogene Informationen betreffend sein Privatleben über ihn ermittelt, verarbeitet, veröffentlicht oder ähnliches werden da sie alle Art 8 EMRK berühren.

¹⁰⁴ *Jahnel*, OGH: Kein Schutz vor Unternehmensdaten im DSG ?, RdW 2005/244, 200ff zur problematischen Entscheidung OGH 4.5.2004, 4 Ob 50/04p; VfSlg 16.369/2001; VfSlg 12.228/1989; VfSlg 12.880/1991

¹⁰⁵ *Felt/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 233 (236) mwN; VfSlg 12.228/1989, 12.880/1991; 16.369/2001; VwGH 30.4.2003, 2001/03/0036

¹⁰⁶ OGH EvBl 2001, 19; zur Zulässigkeit der Übermittlung von Einkommensdaten an die Sozialversicherung, VfGH 2.10.2006, G 29/06

¹⁰⁷ VfSlg 12.880/1991

¹⁰⁸ So *Wiederin*, Privatsphäre und Überwachungsstaat, 60 (FN 298); *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000; aA *Dohr/Pollirer/Weiss*, DSG², § 1 Anm 7, 21

2.7.2.1. Arten von personenbezogenen Daten

Das DSG 2000 kennt folgende Arten von personenbezogenen Daten die sich aufgrund ihrer Schutzwürdigkeit unterscheiden lassen: (abgestuft)^{109 110}

- *Sensible Daten:*¹¹¹ Besonders schutzwürdige („*sensible*“) Daten iSd § 4 Z 2 DSG 2000 von natürlichen Personen sind Daten über die rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben. Da es sich hierbei um eine taxative Aufzählung handelt, fällt der Begriff „*Bonität/Kreditwürdigkeit*“ ebenso wenig darunter wie die Einkommenshöhe obwohl beides zum Bereich des Privatlebens zählt und vom Grundrecht auf Geheimhaltung umfasst sind, wenn nicht besondere Umstände eine Ausnahme statuieren.¹¹² Da die strenge Aufzählung eine Lockerung ausschließt, zeigt jedoch in der Datenschutzpraxis, dass manchmal sonstige, nicht als sensible genannte Daten, aber aus Interessenslage der Betroffenen nicht minder problematische Datenarten, schärfere Verwendungsbeschränkungen erfordern, die auch das Niveau des Schutzes sensibler Daten erreichen können.¹¹³
- *Strafrechtlich relevante Daten:* Sie sind zwar keine sensiblen Daten aber für sie gelten besondere Bestimmungen hinsichtlich der Zulässigkeit der Verwendung (§ 8 Abs 4 DSG 2000) und hinsichtlich der Vorabkontrolle (§ 18 Abs 2 Z 2 DSG 2000)
- Daten über die *Kreditwürdigkeit*, Informationsverbundsysteme
- *Bestimmte oder bestimmbare personenbezogene Daten* (nicht-sensible Daten): Darunter sind gem § 4 Z 1 DSG 2000 Angaben über Betroffene zu verstehen, deren Identität bestimmt oder bestimmbar ist.
- *Indirekt personenbezogene Daten* sind Daten, bei denen der Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann. Sie werden als weniger schutzwürdig angesehen und genießen gewisse Erleichterungen zB bei der Zulässigkeit der Verwendung (§§ 8 Abs

¹⁰⁹ Aufstellung nach *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, 317ff; *derselbe* in Aktuelle Fragen des DSR, 81

¹¹⁰ Je höher die Schutzwürdigkeit, umso höher auch die Anforderungen an die Datensicherheitsmaßnahmen

¹¹¹ Ausführlich hiezu *Jahnel*, Begriff und Arten von personenbezogenen Daten in Jahrbuch Datenschutzrecht und E-Government, 40ff

¹¹² DSK 6.5.1998, ZfVB 1998/5, 755

¹¹³ Vgl § 18 Abs 2 DSG 2000 betreffend die Vorabkontrolle bestimmter Anwendungen; *Duschanek* § 1 DSG 2000 in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, Rz 29

2 und 9 Z 2 DSG 2000), Übermittlung und Überlassung in das Ausland (§ 12 Abs 3 Z 2 DSG 2000)

- *Anonymisierte Daten*:¹¹⁴ Angaben die nicht auf eine Person rückführbar sind¹¹⁵ stellen überhaupt keine Daten iSd DSG 2000 dar

2.7.2.2. Beschränkungen des Grundrechts

Das Grundrecht auf Datenschutz wirkt nicht absolut, sondern kann durch bestimmte nach § 1 Abs 2 DSG 2000 zulässige Eingriffe beschränkt werden. Dies gilt sowohl für das Grundrecht auf Geheimhaltung als auch für die Grundrechte auf Auskunft, Richtigstellung und Löschung iSd § 1 Abs 3 DSG 2000.

§ 1 Abs 2 DSG 2000 normiert vier verschiedene Fälle in denen Beschränkungen des Grundrechts zulässig sind:

- Verwendung im lebenswichtigen Interesse des Betroffenen
- Verwendung mit seiner Zustimmung
- zur Wahrung überwiegend berechtigter Interessen eines anderen¹¹⁶
- Wahrung überwiegenden berechtigter (wichtiger öffentliche) Interessen des Staates nur aufgrund von Gesetzen in Einklang mit Art 8 Abs 2 EMRK (materieller Gesetzesvorbehalt)

Liegt einer der o.a. Rechtfertigungsgründe vor, so wird aus der Eingriffshandlung welche zunächst eine Grundrechtsverletzung darstellt, ein zulässiger Eingriff. Während bei manchen Grundrechten mit dem Vorliegen der Zustimmung ein Eingriff bereits ausgeschlossen wird,¹¹⁷ ist dies beim Grundrecht auf Datenschutz nicht der Fall.¹¹⁸ Eine Zustimmung (zur Zustimmung siehe Kapitel 6.2.2.) rechtfertigt nur den Eingriff, es sei denn, der Veröffentlichung von Daten wird zugestimmt. Dann wird der Grundrechtsschutz *ex nunc*

¹¹⁴ Schwierig wird die Abgrenzung bei „totaler A.“ und „faktischer A.“ => eine Reidentifikation ist zwar möglich aber aufgrund der Umstände des Einzelfalls äußerst unwahrscheinlich – hierzu *Löschnigg*, Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459 (461)

¹¹⁵ RV 1613 BlgNR XX.GP 37; ebenso *Jahnel*, Das DSG 2000. Wichtige Neuerungen, wbl 2000, 45 (51)

¹¹⁶ Wobei nicht nur Interessen von Privaten sondern auch Interessen juristischer Personen des öffentlichen Rechts verstanden werden sowie siehe Punkt 4

¹¹⁷ *Berka*, Grundrechte, Rz 178; für das Fernmeldegeheimnis, *Himberger*, Fernmeldegeheimnis, 71

¹¹⁸ AA *Geiger*, NVwZ 1989, 36ff – der für die deutsche Rechtslage – davon ausgeht, dass die Einwilligung eine Ausübung des Rechts auf informationelle Selbstbestimmung und damit Grundrechtsausübung ist und nicht Grundrechtsverzicht

langfristig beseitigt und in diesen Fällen liegt dann für die zukünftigen „Eingriffe“ gar kein Eingriff mehr vor, weil die Daten allgemein verfügbar sind iSd § 1 Abs 1 DSG 2000.¹¹⁹ Berka¹²⁰ sieht in der Zustimmung geradezu eine Paradebeispiel des freien Grundrechtsgebrauchs. Die häufigsten Fälle der Zustimmung haben ihrer Grundlage in der Drittwirkung des Grundrechts gegenüber Privaten und beruhen auf zivilrechtlichen Verträgen im Rahmen der Privatautonomie der Beteiligten.

Bei der Beschränkung der Geheimhaltung zugunsten anderer Interessen ist daher immer eine Interessenabwägung mit den schutzwürdigen Geheimhaltungsinteressen des Betroffenen anzustellen, und zwar sowohl bei Eingriffen zugunsten widerstreitender Privatinteressen als auch in der Verfolgung öffentlicher Interessen.¹²¹

Eingriffe jedoch müssen nicht unbedingt die Form eines individuellen Rechtsaktes bekleiden. Bereits die Geltung eines Gesetzes kann einen Eingriff darstellen, wenn seine Adressaten lediglich die Wahl haben, die verbotene Betätigung zu unterlassen oder sich der Gefahr strafrechtlicher Verfolgung auszusetzen. Nach der Rechtsprechung des EGMR gilt dies unabhängig davon ob die betroffenen Personen je das Objekt konkreter behördlicher Maßnahmen waren oder ob das Gesetz in der Praxis angewendet wurde.¹²²

Als Eingriffsgrund sind nur „berechtigte“ Interessen anerkannt welche rechtlich abgesichert sind und zwar entweder dass die Datenverwendung von der Rechtsordnung angeordnet oder anerkannt ist oder dass die Daten für die Durchsetzung eines Rechtsanspruches benötigt werden.¹²³

Damit wird bei der Beschränkung des Grundrechts tlw beim Eingriffssubjekt unterschieden:

Bei der Legitimierung des Grundrechtseingriffs durch ein überwiegendes berechtigtes Interesse eines anderen der nicht durch staatliche Behörden erfolgt, wird die überwiegende Interessenslage auch bei Eingriffen in sensible Daten nicht näher ausgeführt.

Bei Eingriffen einer staatlichen Behörde ist diese jedoch bestimmten, inhaltlichen Schranken („*Schranken-Schranken*“) unterworfen und darf diese nur mit den gelindesten Mitteln (auch „*zielführendes Mindestmaß*“) durchführen. Es handelt sich um einen „*materiellen Gesetzesvorbehalt*“ mit einer taxativen Aufzählung zulässiger Eingriffsgründe, normiert in Art 8 Abs 2 EMRK. Damit wird das nach der Judikatur und der Grundrechtsdogmatik

¹¹⁹ Zu einem möglichen „Wiederaufleben“ des Grundrechtsschutzes, Reimer, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung in Jähnel/Siegrwart/Fercher, Aktuelle Fragen des Datenschutzrechts, 188

¹²⁰ Duschaneck, § 1 DSG 2000 in Korinek/Holoubek (Hrsg), Österr BVfR – GR III, Rz 46

¹²¹ Duschaneck, § 1 DSG 2000 in Korinek/Holoubek (Hrsg), Österr BVfR – GR III, Rz 48

¹²² EGMR 20.10.1981, Fall *Dudgeon*, Z 41

¹²³ Matzka, § 1 K 8; Dohr/Pollirer/Weiss, § 1 Anm 10, 13; Drobosch/Grosinger, 99; auch OGH 27.9.1988, 4 Ob 581/88 (Einkommenserhebung zur Unterhaltsbemessung)

bestehende Verhältnismäßigkeitsgebot auch für das Grundrecht auf Datenschutz festgeschrieben. Grundrechtseingriffe durch staatliche Behörden, die sich auf keinen der in Art 8 Abs 2 EMRK genannten Gründe berufen können oder damit in Widerspruch stehen, wären auch dann verfassungswidrig wenn sie eine einfachgesetzliche Grundlage aufweisen.¹²⁴ Die Einrichtung und der Betrieb von öffentlichen Registern¹²⁵ oder veraltungsinterner Evidenzen¹²⁶ bedeutet ebenfalls eine Beschränkung des datenschutzrechtlichen Geheimhaltungsanspruches und muss daher den Anforderungen des § 1 Abs 2 DSG 2000 entsprechen. Bei Eingriffen in sensible Daten müssen darüber hinaus die Wichtigkeit des Eingriffes nachgewiesen und angemessene Garantien für den Geheimnisschutz vorgesehen werden.¹²⁷

Der VfGH hat in seiner Judikatur wiederholt betont, dass Eingriffe in das Grundrecht auf Datenschutz einer ausreichend bestimmten gesetzlichen Grundlage bedürfen und Versuche staatsnaher Betriebe diesbezüglich als verfassungswidrig zurückgewiesen.¹²⁸

Gemäß § 1 Abs 4 DSG 2000 sind schließlich auch Beschränkungen der Leistungsansprüche auf Auskunft, Richtigstellung und Löschung nur unter den in Abs 2 genannten Voraussetzungen zulässig und unterliegen daher ebenfalls der Verhältnismäßigkeit.¹²⁹

Wer jedoch den Datenschutz zu „kleinen Münze“ entwertet und jede Datenerfassung oder Verwendung von Daten unabhängig von ihrer Schutzwürdigkeit als Eingriff in das Grundrecht ansieht, trägt möglicherweise mehr zur Entwertung des Grundrechts bei, als wenn man sich auf die wirklich erheblichen Eingriffe konzentriert und hier versucht, die Eingriffsschwelle entsprechend hoch anzusetzen.¹³⁰ Als Beispiel sei hier die Entscheidung des OGH bezüglich der *Überwachung des Telefonverkehrs in Betrieben* genannt wo dieser eine Beeinträchtigung der Menschenwürde erkannte obwohl die gewählte Rufnummer bei privaten

¹²⁴ VfSlg 16.369/2001, *Berka*, Grundrechte, Rz 258, *Wiederin*, Art 8 EMRK, Rz 17, 21 beide in *Korinek/Holoubek* (Hrsg), Österr BfVR – GR III

¹²⁵ zB Wählerevidenz, Melderegister, Gewerberegister, Vereinsregister, Chemikalienregister, etc

¹²⁶ zB die zentrale Inforationssammlung („EKIS“) gem §§ 57ff SPG, Zentrale Zulassungsevidenz gem § 47 Abs 4 KFG

¹²⁷ *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, 327f

¹²⁸ Zur Sammlung von Wirtschaftsdaten der Telekom Control VfSlg 16.369/2001; zur Section Control VfGH 15.6.2007, G 147/06; ferner VfSlg 12.166/1989, 16.467/2002; zur Judikatur des EGMR 4.5.2000, *Rotaru/Rumänien*, Nr. 28.341/95, ÖJZ MRK 2001, 74 sowie *Wiederin*, Art 8 EMRK in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, Rz 16; *Grabenwarter*, EMRK² (2005), 180, 192

¹²⁹ *Duschanek*, § 1 DSG 2000 in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, Rz 61, 79, 85

¹³⁰ *Berka*, Geheimnisschutz-Datenschutz-Informationsschutz im Lichte der Verfassung, 64ff

Telefonaten ohnedies unterdrückt wurde; vor allem dann wenn wir die Menschenwürde als oberste Maxime der Rechtsordnung anerkennen.¹³¹

¹³¹ OGH SZ 2002/83

2.7.3. Österreichisches Verfassungsrecht und EMRK

Art 8 EMRK lautet:

(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.*¹³²

Obwohl Art 8 EMRK ebenfalls im Verfassungsrang steht entfaltet es nach Kommission und EGMR keine Drittwirkung.¹³³ Nur natürliche Personen haben einen Anspruch auf Achtung des Art 8 EMRK. Juristische Personen u.ä. scheiden als Grundrechtsträger aus.¹³⁴

Im Vergleich zum der Grundrechtstatbestand des § 1 DSG 2000 reicht dieser über Art 8 EMRK hinaus, weil er sich auf jede Datenverwendung durch Private sowie den Datenschutz juristischer Personen erstreckt und überdies komplementäre Ansprüche des Betroffenen auf Auskunft, Richtigstellung und Löschung vorsieht.¹³⁵ Im Vergleich zum „schutzwürdigen Geheimhaltungsinteresse“ des § 1 DSG 2000 besteht insofern der Unterschied, dass eine Verarbeitung öffentlich zugänglicher Informationen sehr wohl einen Eingriff in das Privatleben darstellen kann obwohl andererseits ein Eingriff in das Grundrecht auf Datenschutz aufgrund des Fehlens der Schutzwürdigkeit der Geheimhaltungsinteressen ausgeschlossen ist.¹³⁶

Der Zusatz „insbesondere auch im Hinblick auf die Achtung des Privat- und Familienlebens“ zeigt bereits das Naheverhältnis des Grundrechts auf Geheimhaltung zur Art 8 EMRK. Dies wird auch durch den Gesetzesvorbehalt in § 1 Abs 2 DSG 2000 zum Ausdruck gebracht, der

¹³² Zu Art 8 Abs EMRK vgl. *Wiederin* in *Korinek/Holoubek* (Hrsg), Österr BVfR, Art 8 EMRK Rz 22ff

¹³³ *Brötel*, Der Anspruch auf Achtung des Familienlebens (1991) 73ff; *Gusy*, Der Schutz der Privatsphäre in der EMRK Art 8, DuR 13 (1984), 289 (297); *Wiederin*, Privatsphäre und Überwachungsstaat (2003), 21

¹³⁴ aA *Potacs*, Devisenbewirtschaftung, 1991, 405ff

¹³⁵ *Wiederin* in *Korinek/Holoubek* (Hrsg), Österr. BVfR, Art 8 EMRK Rz 136; *Wildhaber*, Art 8 EMRK in *Karl* (Hrsg) Internationaler Kommentar zur Europäischen Menschenrechtskonvention, Rz 323ff mit ausführlichen Judikaturhinweisen

¹³⁶ *Wiederin*, Privatsphäre und Überwachungsstaat (2003), 59

auf Art 8 Abs 2 EMRK verweist. Der EGMR leitet in seiner Judikatur aus Art 8 EMRK auch ein Recht auf Datenschutz ab.¹³⁷ Eine genaue Definition des Begriffes „*Privatleben*“ ist oft versucht aber nie endgültig erreicht worden.¹³⁸ Auch der EGMR hält eine erschöpfende Begriffsbestimmung für unmöglich¹³⁹ und beurteilt von Fall zu Fall ob ein Eingriff vorliegt oder nicht. Die hL hält es weitgehend für ausgemacht, dass der Begriff Privatleben über „privacy“ hinausgeht und daher nicht auf die Abgeschlossenheit der eigenen Sphäre reduziert werden kann, sondern auch die menschliche Persönlichkeit selbst in ihrer Identität, Individualität und Integrität unter Schutz stellt.¹⁴⁰

Obwohl der EGMR sich nicht am dreistufigen Verhältnismäßigkeitsschema von *Tauglichkeit* – *Erforderlichkeit* – *Verhältnismäßigkeit* im engeren Sinn orientiert, dominieren doch die Gemeinsamkeiten.¹⁴¹ Entscheidend ist jedoch, dass der Eingriff in Hinblick auf das verfolgte Ziel sich als *angemessen* erweist.¹⁴²

Der EGMR lässt sich dabei von folgenden Grundsätzen leiten:

- Notwendigkeit bedeute nicht Unentbehrlichkeit der Regelung; diesem Kriterium wohnt jedoch nicht die Flexibilität der Begriffe „normal“, „nützlich“ oder angemessen inne¹⁴³
- Die Schrankenvorbehalte müssen eng ausgelegt werden. Denn Kennzeichen einer demokratischen Gesellschaft sind Großzügigkeit und Toleranz¹⁴⁴
- Das Kriterium der „Notwendigkeit“ erfordert den Eingriff aufgrund eines dringenden sozialen Bedürfnis sowie dessen angemessenen Verhältnis zum verfolgten Ziel¹⁴⁵
- Die Vertragsstaaten verfügen über einen gewissen aber nicht unbeschränkten Ermessensspielraum und sie müssen das Vorliegen eines dringenden sozialen

¹³⁷ Wiederin in *Korinek/Holoubek* (Hrsg), Österr. BVfR, Art 8 EMRK Rz 51

¹³⁸ Vgl hierzu Evers, EuGRZ 1984, 290; Ruiz, Privacy in Telecommunications (1997), 43ff

¹³⁹ EGMR Fall *Costello-Roberts gegen Vereinigtes Königreich*, Serie A Nr 247-C = ÖJZ 1991, 707 (Z36); Fall *Raninen gegen Finnland*, RJD 1997-VIII, 2804, Z 63; Fall *Peck gegen Vereinigtes Königreich*, Appl 44.647/98, Z 57; *Velu*, Private Life, 36ff; *Villiger*, Handbuch, Rz 555

¹⁴⁰ *Berka*, Grundrechte Rz 457; Evers, 285; *Kopetzki*, Unterbringungsrecht (1995), *Lukasser*, EMRK und individueller Lebensstil, ÖJZ 1994, 569 (570)

¹⁴¹ *Berka*, Die Gesetzesvorbehalte der EMRK, ZÖR 37, 1986/87, 71; *Stelzer*, Das Wesensgehaltsargument und der Grundsatz der Verhältnismäßigkeit, 1991, 274ff; *Wiederin*, Art 8 EMRK in *Korinek/Holoubek*, BVfR-GR III, 21; *Fahrenhorst*, Familienrecht und EMRK, 159ff

¹⁴² EGMR, Fall *Olsson I* (FN 75), Z 67

¹⁴³ EGMR, Fall *Dudgeon*, Z 51; Fall *Silver* (FN 77), Z 97, jeweils mwN

¹⁴⁴ EGMR, Fall *Dudgeon*, Z 53; eingehend auch *Berka*, Die Gesetzesvorbehalte der EMRK, 91ff

¹⁴⁵ EGMR, Fall *Dudgeon*, Z 51+53; Fall *Silver*, Z 97

Bedürfnisses einschätzen. Der EGMR soll diese Bewertung nicht durch eine andere ersetzen.¹⁴⁶

- Der EGMR hat eine objektive Beurteilung abzugeben; er darf seine Kontrolle nicht darauf beschränken, ob der betroffene Mitgliedsstaat sein Ermessen sachgerecht, sorgfältig und in gutem Glauben ausgeübt hat¹⁴⁷
- Ein europäischer Standard auf einem bestimmten Politikfeld wird vom EGMR registriert und impliziert prima facie, dass Abweichungen problematisch sind. Dabei können jedoch internationale und nationale kulturelle und sonstige Unterschiede bestehen die sich in unterschiedlichen gesellschaftlichen Anforderungen niederschlagen und Sonderregelungen rechtfertigen mögen.¹⁴⁸
- Je schwerer ein Eingriff und je persönlicher die berührenden Interessen, umso überzeugender muss seine Notwendigkeit dargelegt werden¹⁴⁹
- Bei der Prüfung ist der Fall als Ganzes zu betrachten und zu beurteilen, ob die zur Rechtfertigung angeführten Gründe einschlägig und ausreichend sind¹⁵⁰
- Der behördliche Entscheidungsprozess hat Einfluss auf die Begründetheit von Entscheidungen und muss daher auf eine Art und Weise organisiert sein, dass alle involvierten Interessen berücksichtigt werden und die Entscheidung weder willkürlich ist noch als solche erscheint. Es muss daher sichergestellt sein, dass die betroffene Person hinreichend Gehör findet und die Entscheidung relativ rasch erfolgt.¹⁵¹
- Sofern eine konkrete individuelle Betroffenheit feststeht bzw. hinreichend als wahrscheinlich erscheint, hängt das Vorliegen eines Eingriffs nicht davon ob diese staatliche Maßnahme in eine Rechtsform gekleidet ist, die dem Betroffenen deren Bekämpfung erlaubt. Auch dann wenn Rechtsmitteln fehlen, liegt ein rechtfertigungsbedürftiger Eingriff vor.^{152 153}

¹⁴⁶ EGMR, Fall *Klass*, Z 49; Fall *Stjerna*, Z 39

¹⁴⁷ EGMR, Fall *Olsson I*, Z 68

¹⁴⁸ EGMR, Fall *Rees*, Z 37; Fall *Cossey*, Z 40, Fall *Stjerna*, Z 39; Fall X, Y und Z, RJD 1997-II,619=ÖJZ 1998 (Z44)

¹⁴⁹ Eingehend *Wildhaber/Breitenmoser*, Human rights, democracy and the rule of law, Rz 680ff; *Villiger*, Handbuch der EMRK, Rz 553

¹⁵⁰ EGMR, Fall *Olsson I*, Z 68

¹⁵¹ EGMR, Fall W Serie A Nr 121=EuGRZ 1990, 553 (Z 62ff); Fall R, Serie A Nr 121, Z 67; Fall *Olsson I*, Z 71; Fall *McMichael*, Z 87+92; 16.9.1999, Fall *Buscemi*, Appl 29.569/95, Z 58; Fall *Elsholz*, Appl 25.735/94=EuGRZ 2001, 595 = ÖJZ 2002, 71 (Z52ff)

¹⁵² Evers, Der Schutz des Privatlebens und das Grundrecht auf Datenschutz in Österreich, EuGRZ 1984, 281 (286)

¹⁵³ Zur damaligen Lücke im Rechtsschutzsystem, VfSlg 9783/1983, 9934/1984, 11.935/1988 sowie *Funk*, Von der „faktischen Amtshandlung“ zum verfahrensfreien Verwaltungsakt, ZfV 1987, 620ff, *derselbe*, Gewaltlose Zwangsakte und Recht auf eine wirksame Beschwerde, EuGRZ 1989, 518 (521), *Mayer*, Die „Normativität“ faktischer Amtshandlungen, FS *Walter* (1991), 463 (468), sowie Bericht des EKMR vom 12.3.1987, Appl 10126/82, Plattform Ärzte für das Leben gg. Österreich

Der VfGH hat sich diesen Grundsätzen angeschlossen wobei er jedoch weiters ausführt, dass der Gesetzgeber durch Art 8 EMRK regelmäßig nicht auf eine einzige „beste“ Lösung festgelegt ist¹⁵⁴ sondern durch die Notwendigkeit in einer demokratischen Gesellschaft ein Handlungsspielraum demokratisch festgelegter Parlamente impliziert.¹⁵⁵ Selbst bei vorliegen eines „europäischen Standards“ verbleibt dem Mitgliedsstaat die Möglichkeit, ein eigenständiges rechtspolitisches Profil zu entwickeln.¹⁵⁶ Der VfGH macht den Schutz des Art 8 EMRK im Ansatz davon abhängig ob das betroffene Verhalten der Öffentlichkeit gegenüber in Erscheinung tritt.¹⁵⁷ Aber er lehnt auch das Vorliegen eines Eingriffs mit der Begründung ab, dass es sich hierbei um Wirtschaftsleben handle.¹⁵⁸ Einer strikten Gegenüberstellung von Berufs- und Privatleben hat er schon frühzeitig eine Absage erteilt um damit der Entscheidung vorzubeugen jedes Handeln welches nicht in Ausübung des Berufes erfolgt, der Intimsphäre des Privat- und Familienlebens zuzurechnen.¹⁵⁹ Auch wenn bestimmte Vorgänge und Umstände nicht geheim gehalten werden können und einem durch die Umstände beschränkten Personenkreis ohne weiteres bekannt werden, ist es doch Sache des Betroffenen zu entscheiden, ob und was er darüber welchen anderen wissen lässt.¹⁶⁰ Daher können öffentliche Anprangerungen wie zB die Bekanntmachung des Namens von Verbrechern, Drogenkonsumenten oder Pleitiers durchaus das Privatleben berühren.¹⁶¹

In seinem Erkenntnis zum „Videotheken-Fall“ betreffend das Wr VergnügungssteuerG, VfGH 14.03.1991, G148-155/90 (VfSlg 12.689/1991, 510) hat der VfGH dieses Grundrecht als Abwehrrecht erkannt. *„In einer von der Achtung der Freiheit geprägten Gesellschaft wie sie die Präambel zur MRK voraussetzt, braucht der Bürger ohne triftigen Grund niemanden Einblick zu gewähren, welchen Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitungen er abonniert, was er isst und trinkt und wo er die Nacht verbringt. Auch wenn solche Vorgänge und Umstände oft nicht eigentlich geheim gehalten und einem durch die Umstände beschränkten Personenkreis ohne weiteres bekannt werden, ist es doch Sache des Betroffenen, zu entscheiden, ob und was er darüber welchen anderen wissen lässt.“*

Das Recht auf „Intimität“ steht zwar im Dienst der Entfaltung der eigenen Persönlichkeit, garantiert diese aber nicht. Autonome Lebensgestaltung wird durch Art 8 EMRK nicht

¹⁵⁴ VfSlg 12.103/1989, 13.629/1993, 14.301/1995

¹⁵⁵ VfSlg 12.103/1989, 13.629/1993

¹⁵⁶ VfSlg 13.629/1993

¹⁵⁷ VfSlg 8272/1978, 8445/1978, 8907/1980, 14.485/1996

¹⁵⁸ VfSlg 10.063/1984

¹⁵⁹ VfSlg 6534/1971

¹⁶⁰ VfSlg 12.689/1991

¹⁶¹ Haefliger/Schürmann, Die EMRK und die Schweiz, 257, mwN

unbeschränkt geschützt, sondern nur insoweit als die eigene Identität und Integrität berührt wird. Ebenfalls nicht erfasst ist die Entscheidung darüber, Informationen ausgesetzt zu werden. Informationskontrolle schützt vor der Neugierde der Öffentlichkeit, erspart aber nicht die Konfrontation mit ihr und bedeutet auch kein Recht auf Zugang von Information. Art 8 EMRK schützt Einflüsse gegenüber der eigenen physischen und psychischen Integrität sowie die eigene Wohnung. Dieses Recht auf Informationskontrolle wirkt aber nicht absolut, denn nicht Erhebung oder Verwendung einer personenbezogenen Information durch den Staat ist per se schon ein Eingriff.¹⁶²

Der Staat darf sich jedoch nicht darauf beschränken Eingriffe in das Recht auf Achtung des Privat- und Familienlebens zu unterlassen, sondern er muss darüber hinaus diese Rechtsgüter auch *aktiv* gewährleisten und sie gegenüber Gefährdungen in Schutz nehmen, die ihm von Seiten anderer Privater drohen.¹⁶³ Den Mitgliedsstaaten stehen dazu verschiedene Wege offen und die Wahl der Mittel grundsätzlich einen Ermessensspielraum beinhaltet. Der Schutz im Wege von Strafvorschriften ist eine wichtige, aber nicht notwendig die einzige in Betracht kommende Möglichkeit.¹⁶⁴

Die Grundrechtsformel anhand der VfGH in ständiger Rechtsprechung in Art 8 EMRK eingreifende Bescheide auf eine Verletzung dieses Grundrechts prüft hat folgende Gestalt:¹⁶⁵ Ein unter Art 8 EMRK verfassungsgesetzlich garantiertes Recht wird dann verletzt wenn

- Der ihn verfügende Bescheid ohne jede Rechtsgrundlage ergangen ist,
- auf einer dem Art 8 EMRK widersprechenden Rechtsvorschrift beruht
- oder wenn die Behörde eine verfassungsrechtlich unbedenkliche Rechtsgrundlage in denkunmöglicher Weise angewandt hat; dies liegt jedoch nur dann vor wenn die Behörde so einen schweren Fehler gemacht hat, dass dieser mit einer Gesetzeslosigkeit auf eine Stufe zu stellen wäre, oder wenn sie den angewandten Rechtsvorschriften fälschlicherweise einen verfassungswidrigen, insbesondere einen dem Art 8 Abs 1 EMRK widersprechenden und durch Art 8 Abs 2 EMRK nicht gedeckten Inhalt unterstellt hat.

¹⁶² Wiederin in *Korinek/Holoubek* (Hrsg), Österr. BVfR, Art 8 EMRK, Rz 36

¹⁶³ EGMR, Fall *Marchx gegen Belgien*, Serie A 21 = EuGRZ 1979,454, Z 31; Fall *X und Y gegen Niederlande*, Serie A 91 = EuGRZ 1985, 297, Z 23; Fall *Botta gegen Italien*, RJD 1998-I, 412 = ÖJZ 1999, 76, Z 33

¹⁶⁴ EGMR, Fall *X und Y gegen Niederlande*, Z 24; Fall *Stubbings gegen Vereinigtes Königreich*, RJD 1996-IV, 1487 = ÖJZ 1997,436, Z 63

¹⁶⁵ VfSlg 13.497/1993, 13.673/1994, 14.009/1995; sowie VfSlg 13.357/1993 und VfSlg 14.542/1996, wonach die fehlerhafte Annahme von Ermessen Art 8 EMRK verletzt

Der EGMR stellt klar, dass er die Anwendung der Datenschutz RL genau nach jenen Kriterien angewendet wissen will, die er seit jeher bei der Anwendung des Art 8 EMRK heranzieht:¹⁶⁶

- Klare Determinierung und Vorhersehbarkeit der Eingriffsvoraussetzungen
- Orientierung an einem legitimen Eingriffsziel
- zwingendes soziales Bedürfnis
- Notwendigkeit des Eingriffs in einer demokratischen Gesellschaft
- Verhältnismäßigkeit der angewendeten Mittel

Durch die Regelungen in der Datenschutz RL 95/46/EG wird zwar der Vorrang des freien Datenverkehrs im Binnenmarkt zugunsten nationaler Datenschutzregelungen manifestiert¹⁶⁷ jedoch auch andererseits wird durch die Bestimmungen in Art 1 Abs 1 der Datenschutz RL das Grundrecht auf Schutz der Privatsphäre im Sinne des Art 8 EMRK ebenso wie weiterer Grundrechte konkretisiert¹⁶⁸. Die DS-RL verpflichtet jedoch die Mitgliedsstaaten nicht zur Schaffung eines Grundrechts auf Datenschutz. Soweit keine Umsetzungsverpflichtung besteht, kann es auch keine richtlinienkonforme Interpretation geben, da diese nicht weiter reicht als die Umsetzungsverpflichtung.¹⁶⁹ Dennoch sind die Begriffe der Verfassungsbestimmung des DSG unter Heranziehung der einfachgesetzlichen Legaldefinitionen in einem richtlinienkonformen Verständnis zu interpretieren.¹⁷⁰

¹⁶⁶ Weh, Der Schutz wirtschaftlicher Daten im europäischen Datenrecht, GesRZ 2003, 322

¹⁶⁷ Art 1 Abs 2 DS-RL lautet: „Die Mitgliedstaaten beschränken oder untersagen nicht den freien Datenverkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Abs 1 gewährleisteten Schutzes“.

¹⁶⁸ Art 1 Abs 1 DS-RL lautet: „Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“. Neben dem Grundrecht auf Datenschutz weisen auch andere Grundrechte, wie zB das Brief- und Fernmeldegeheimnis, das Hausrecht, die Meinungsäußerungsfreiheit datenschutzrechtliche Bezüge auf (vgl. Duschanek, Neuerungen und offene Fragen im DSG 2000; Dammann/Simitis, EG DS-RL, Kommentar (1997), 101

¹⁶⁹ Wiederin, Privatsphäre und Überwachungsstaat, 58; aA Duschanek, § 1 DSG 2000, Rz 17

¹⁷⁰ Jahnel, Das Grundrecht auf Datenschutz nach dem DSG 2000 in FS Schäffer, 317

3. Bonität/Kreditwürdigkeit

Aber auch schon der Begriff der „Bonität/Kreditwürdigkeit“ erfordert eine nähere Betrachtung und Definition weil es sich hierbei schließlich um die „andere Seite“ des Begriffspaares handelt. Im negativen Sinn betrachtet kann man auch von „Kreditrisiko“ sprechen. Dh die Wahrscheinlichkeit dass es zu Zahlungsproblemen, teilweisen oder vollständigen Zahlungsausfällen kommt.

Die Kreditwürdigkeit lässt sich im engeren Sinn als Summe der persönlichen Eigenschaften des Kreditnehmers und im weiteren Sinn in die Kreditfähigkeit als seine sachliche (materielle) Potenz, den Kredit vereinbarungsgemäß zurückzuzahlen, bezeichnen.¹⁷¹ Der Kredit im eigentlichen Sinn wird als Überlassung von Geld(kapital) im Vertrauen auf die vereinbarungsgemäße Rückzahlung und Verzinsung, verstanden. Derartiger Kredit wird in Form des Geldkredits, insbesondere Bankkredit oder auch als Warenkredit, nämlich bei dem Bezug von Waren gegen Stundung des Kaufpreises bis zum Absatz der Ware (Lieferantenkredit) gewährt.¹⁷² Für beide Bereiche – Geld- und Warenkredit – bleibt festzuhalten, dass die persönliche Zuverlässigkeit des Kreditnehmers für seine Kreditwürdigkeit ausschlaggebend ist. Das wirtschaftliche Schicksal eines Betriebes richtet sich überwiegend nach den Fähigkeiten seiner Leitung, so dass das Vertrauen in diese Fähigkeiten regelmäßig die wesentliche Voraussetzung für die Kreditgewährung darstellt und wird daher folgerichtig eine eingehende Kontrolle auch der Persönlichkeitsstruktur der Kreditanwärter empfohlen.¹⁷³

3.1. Das Kreditrisiko

Das Kreditrisiko lässt sich grundsätzlich in das *aktive Kreditrisiko* und das *passive Kreditrisiko* gliedern.

Das *aktive Kreditrisiko* wird in Bonitäts-, Besicherungs- und Liquiditätsrisiko untergliedert und umfasst im weiteren Sinn die Kreditfähig- und Würdigkeit (d.h. das Risiko fristgerechter Kreditrückführung)

Das *passive Kreditrisiko* beinhaltet für den Kreditgeber die Unsicherheit, dass die Refinanzierungsmittel (z.B. bei Kreditinstituten die Spareinlagen) vor deren Fälligkeit rückgeführt werden müssen.

¹⁷¹ Hagenmüller, Der Bankbetrieb, 275; Tiedemann, Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft, 5

¹⁷² Tiedemann, (FN 53), 1; W.Kalveram, Bankbetriebslehre, 24 sowie Die Prüfung der Kreditwürdigkeit, 6

¹⁷³ Hagenmüller (FN 53), 276, Mellerowicz-Jonas, Bestimmungsfaktoren der Kreditfähigkeit, 15, 19ff

Interessant in diesem Zusammenhang ist nur das *aktive Kreditrisiko*.

Jeder vernunftbegabte Kaufmann wird vor Abschluss eines Geschäftes eine Risikoprüfung durchführen um das Kreditrisiko zu erkennen, zu beurteilen und dieses in einem vernünftigen Verhältnis zum Ertrag zu kalkulieren. Obwohl Banken über die eigenen Kunden sicher die beste Übersicht über deren wirtschaftliches Gebaren haben, so werden doch auch von diesen Auskünfte von Auskunftgebern eingeholt wenn ein neuer, noch unbekannter Kunde Kredit begehrt. Durch eine zusätzliche kollektive Kreditkontrolle in Gestalt von Bankenkooperationen, Gläubigerschutzverbänden und teilweise Meldepflichten der Kreditinstitute soll verhindert werden, dass der Kreditnehmer die im jeweiligen Einzelfall vorhandene Kreditfähigkeit bei verschiedenen Kreditinstituten/Lieferanten mehrfach ausschöpft und damit in weiterer Folge ungesicherte und möglicherweise auch riskante Kredit erlangt.

Natürlich handelt es sich nicht stets um nachweisbares strafrechtlich relevantes Verhalten, sondern um teilweise nur unseriöses, aber doch wirtschaftlich gefährliches Verhalten. *Zirpins*¹⁷⁴ schlägt daher vor, diese Verhaltensweise mit dem Begriff „wirtschaftsdelinquentes Verhalten“¹⁷⁵ zu bezeichnen, *„die dem Gebaren und der Vorstellung eines ordentlichen Kaufmanns von Anstand und Sitte im Geschäftsleben widersprechen und die nach Tatausführung und –auswirkung geeignet sind, über eine Schädigung von Einzelinteressen hinaus das Wirtschaftsleben oder die Wirtschaftsordnung zu gefährden“*.

Die Erstprüfung erfolgt vor der Entscheidung zwischen Geschäftsleuten/-partnern bei großen Beträgen/Finanzierungen anhand von Analyse von Bilanzkennzahlen von Jahresabschlüssen und/oder offene bzw. gewährte Kredite im weiteren Sinn, sodann der Beurteilung des Vertragspartners/Kreditnehmers der Kreditfähigkeit allgemein etwa aufgrund persönlicher Daten, Zahlungserfahrungen, Management, Marktlage, Konkurrenz sowie durch eine Subsummierung alle oben angeführten Informationen im Sinne einer Prognose.¹⁷⁶

3.2. Die Kreditprüfung/Kreditanalyse

¹⁷⁴ *Zirpins*, Kriminalstatistik 1972, 186

¹⁷⁵ darunter versteht *Tiedemann* den Geld- und Warenkreditbetrug, Schwindelfirmen mit betrügerischer Absicht sowie Insolvenzen (Konkurs- und Ausgleich), in *Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft*, 8ff

¹⁷⁶ Schwarz, ÖBA 8/01, S 611 ff

Die Kreditprüfung bzw. auch Kreditanalyse/-überwachung geht von der hL von den fünf „C’s“ aus:¹⁷⁷

1. Character: die Einschätzung des Managements hinsichtlich seiner Seriosität
2. Capacity: die Managementfähigkeit zur Aufrechterhaltung der Liquidität und das Erzielen eines nachhaltigen Zukunftsgewinns
3. Capital: die Vermögenslage
4. Collateral: rechtliche und wirtschaftliche Beurteilung der Sicherheiten
5. Conditions: konjunkturelle und technische Bedingungen innerhalb einer Branche und mit Blick auf die gesamte Volkswirtschaft

Im umgekehrten Fall spricht man von „KreditUNwürdigkeit“ wenn die Person/Gesellschaft von dritter Seite zu marktüblichen Bedingungen keinen Kredit mehr erhalten kann und ohne Zuführung von frischem Kapital liquidiert/Insolvenz anmelden müsste.¹⁷⁸ *Schmoll* nennt Kreditnehmer kreditfähig wenn sie wirtschaftlich in der Lage sind einen Kredit zurückzuzahlen und kreditwürdig wenn sie willens sind dies auch zu tun.¹⁷⁹

Natürlich ist hier eine Einzelfallbeurteilung notwendig und es muss geprüft werden ob sich ein wirtschaftlich vernünftig handelnder Drittgläubiger in Kenntnis der Lage anders als der Gesellschafter verhalten hätte und nicht bereit gewesen wäre, der Gesellschaft zu denselben Bedingungen Kredit zu gewähren.¹⁸⁰ Entscheidend ist daher die objektive Würdigung der konkreten wirtschaftlichen Situation im Zeitpunkt der Kreditgewährung. Besonderes Augenmerk ist dabei auf gesellschaftsbezogene Kriterien wie Ertragskraft, Bilanzansätze, verfügbare Sicherheiten, Finanzpläne und auf kreditbezogene Kriterien wie Umfang, Laufzeit, Verzinsung und die Art der Besicherung des Darlehens zu legen.¹⁸¹

Auch im Bereich der Bilanzanalyse unterscheidet man zwischen „hard facts“ worunter man die direkt aus der Bilanz ablesbaren Messgrößen wie Cash flow, Betriebsergebnis, Eigenkapital, Jahresüberschuss versteht und „soft facts“ welche nicht direkt aus der Bilanz ableitbar sind und der individuellen Beurteilung des Kreditanalysten wie z.B. Qualität des Managements, Branchenaussichten, Konkurrenzsituation und Konjunkturabhängigkeit unterliegen. Seit einiger Zeit wird die Bilanzanalyse im Bank- und Kreditgewerbe durch die

¹⁷⁷ B. Zellweger, Überwachung kommerzieller Bankkredite, Bankwissenschaftliche Forschung, Band 77, (1982), 11 ff

¹⁷⁸ OGH 8.5.1991, SZ 64/53 sowie BGH 24.3.1980 BGHZ 76, 330; ZIK 1995/1, 3

¹⁷⁹ *Schmoll*, Theorie und Praxis der Kreditprüfung, 8

¹⁸⁰ P. Bydlinski, Bürgschaft 90 ff; Nowotny, ÖBA 1994, 679; Lutter/Hommelhoff, GmbHG, 14. Aufl., §§32a/b Rz 21; Karsten Schmidt, Kapitalersetzende Bankkredite ?, ZHR 147 (1983) 165, 188 f

¹⁸¹ OGH 8.5.1991 wbl 1991, 400 (*Ostheim*)

Kontodatenanalyse (Soll- und Habenumsätze in Vergleichsjahren, Mahnungen, Rückbuchungen, etc.) ergänzt und kombiniert wodurch noch eine größere Aussagekraft über die Bonität entsteht. Wodurch die Bonitätsprüfung sich in drei Informationsfelder unterscheiden lässt:¹⁸²

- a) vom Unternehmen stammende Unterlagen wie z.B. Bilanzen
- b) innerhalb des kreditgebenden Unternehmens wie z.B. Kontodatenanalyse
- c) Informationen von „Dritten“ wie z.B. Auskunftfeien

Die herrschende Lehre und Rechtsprechung erlaubt, dass zur Aufrechterhaltung der Funktionsfähigkeit der kreditgewährenden Wirtschaft die Mitteilung von negativen Tatsachen und Werturteilen erforderlich ist, und zwar auch von solchen, „denen einseitig die Meinung des Gläubiger zugrunde liegt“.¹⁸³ Im Falle von bestimmten Merkmalen, die üblicherweise als „harte Bonitätsinformationen“ bezeichnet werden können wie z.B. Insolvenzeröffnung, abgelegtes Vermögensverzeichnis, Exekutionen erachtet sie das Interesse an der Übermittlung und der Speicherung regelmäßig überwiegend gegenüber entgegenstehender Persönlichkeits- und Geheimhaltungsinteressen. Eine Güterabwägung ist in diesem Falle daher nicht notwendig. Etwas anders liegt die Sachlage bei „weichen Bonitätsinformationen“ wie z.B. Inkassoaufträge, Kreditkündigungen, Einleitung eines gerichtlichen Verfahrens, etc. Obwohl sicherlich festgestellt werden muss dass auch diese Daten einen gewissen Informationswert über die Bonität eines Kunden besitzen, muss hier eine Einzelprüfung in Hinsicht auf die Verhältnismäßigkeit durchgeführt werden welche einerseits auf die schutzwürdigen Interessen des Betroffenen Rücksicht nimmt als auch auf das berechnigte Interesse des Auftraggebers oder der Allgemeinheit.

3.3. Die Offenlegungspflichten von Kapitalgesellschaften

In diesem Zusammenhang sei auch auf die Offenlegungspflicht für Kapitalgesellschaften verwiesen welche in den §§ 277 ff UGB festgeschrieben ist. Die Offenlegungspflicht bedeutet, dass Kapitalgesellschaften ihren Jahresabschluss, den Lagebericht sowie einen allfälligen Corporate Governance-Bericht beim Firmenbuchgericht zu hinterlegen.¹⁸⁴

¹⁸² Hackl/Schmoll, Kontodatenanalyse zur Früherkennung von Kreditrisiken, ÖBA 11/90, 870 ff

¹⁸³ Gola, Betrieblicher Datenschutz, 90

¹⁸⁴ Auf genauere Ausführungen bezüglich der Hinterlegungspflicht muss hier verzichtet werden

Wie bereits oben (siehe Kapitel 2.7.1.) erwähnt, sind auch wirtschaftsbezogene Daten juristischer Personen nach § 1 DSG 2000 geschützt. Der Gesetzgeber ist jedoch im Sinne des Gläubigerschutzes unter Abwägung der gegenläufigen Interessen dazu berechtigt, Ausnahmen zu statuieren. Dies kann er ja auch beim Anspruch natürlicher Personen auf Achtung des Privat- und Familienlebens, der Wohnung oder des Briefverkehrs nach Art 8 Abs 2 MRK etwa aus dem Grund des wirtschaftlichen Wohls des Landes oder zum Schutz der Rechte und Freiheiten anderer.

Die Hinterlegungspflicht ist weder unverhältnismäßig, noch verletzt sie das Gebot des gelindesten Mittels. Dem Sachlichkeitsgebot und dem Gleichbehandlungsgebot wird mit der Differenzierung des Umfangs der Offenlegungspflicht je nach Größe der Gesellschaft Rechnung getragen. Der verfassungsrechtliche Gleichheitssatz ist nicht darauf gerichtet, alle in der menschlichen Gesellschaft oder im Wirtschaftsleben auftretenden Ungleichheiten zu vermeiden; er soll vielmehr verhindern, dass die Rechtsordnung in unsachlicher Weise differenziert und Rechtsfolgen gleicher (vergleichbarer) Sachverhalte unterschiedlich gestaltet.¹⁸⁵ Der OGH konnte auch keine Rechtswidrigkeit in Umsetzung der „Publizitäts RL“¹⁸⁶ und „Bilanz RL“¹⁸⁷ gegenüber den österreichischen Offenlegungsvorschriften erkennen.¹⁸⁸ Eine Primärrechtswidrigkeit der RL wegen eklatanter Verletzung von Grundrechten (Gleichbehandlung vor dem Gesetz, Grundrecht auf Privatautonomie, Erwerbsfreiheit, Unverletzlichkeit des Eigentums, Recht auf Privatsphäre, Geheimnisschutz, Datenschutz) oder eine allfällige Derogation der RL durch später normiertes Gemeinschaftsrecht hätte der EuGH wahrgenommen und hat in der Entscheidung „Daihatsu“¹⁸⁹ den präjudiziellen Charakter seiner Entscheidung zum Ausdruck gebracht. Art 3 der Publizitäts RL sieht die Führung eines öffentlichen Registers vor, in das alle offen zulegenden Urkunden und Angaben einzutragen sowie für jedermann die Möglichkeit vorsieht, Abschriften der Jahresabschlüsse zugesandt zu bekommen. Dieses Bestreben kommt auch in den Begründungserwägungen der Bilanz RL zum Ausdruck, in denen auf das Erfordernis hingewiesen wird, hinsichtlich des Umfangs der zu veröffentlichenden finanziellen Angaben in der Gemeinschaft gleichwertige rechtliche Mindestbedingungen für miteinander in Wettbewerb stehende Gesellschaften herzustellen. (Erwägungsgrund 22)

¹⁸⁵ Berka, Die Grundrechte, Grundfreiheiten und Menschenrechte in Österreich, Rz 890 ff

¹⁸⁶ Erste gesellschaftsrechtliche Richtlinie des Rates vom 9.3.1968, 68/151/EWG, ABIEG L 65 vom 14.3.1968, 8; anfänglich hatte diese RL Gesellschaften mit beschränkter Haftung von der Offenlegung der Bilanz und GuV Rechnung ausgenommen.

¹⁸⁷ Vierte gesellschaftsrechtliche Richtlinie des Rates vom 25.7.1978, 78/660/EWG, ABIEG L 222 vom 14.8.1978, 11 welche wiederum auf Art 44 Abs 2 lit g EG beruhen; mit dieser RL wurde die Offenlegung auch für Gesellschaften mit beschränkter Haftung normiert

¹⁸⁸ Siehe hiezu OGH 15.12.1999 6 Ob 307/99m; OGH 9.3.200 6 Ob 5/00d; OGH 9.3.2000 6 Ob 14/00b

¹⁸⁹ E 4.12.1997 Slg 1997 I-6843 (Daihatsu); RdW 1998, 525 ff

Das Grundrecht auf Datenschutz ist durch die Offenlegung nicht beeinträchtigt, weil schon kein schutzwürdiges Interesse an der Geheimhaltung des Jahresabschlusses besteht. Die Funktion des Jahresabschlusses besteht ja gerade in der Information der Gesellschafter und auch Dritter. Dementsprechend ist die in der Publizitäts RL und Jahresabschluss RL verlangte Offenlegung nur eine sachlich mit der grundrechtlich gebotenen Interessensabwägung vorgenommene, zum Schutz dritter Personen gebotene Einschränkung des Geheimhaltungsinteresses.¹⁹⁰

Die Behauptung der Verletzung von verfassungsgesetzlich gewährleisteten Rechten durch die Vorschreibung der Zwangsstrafe (siehe oben) kommt der OGH auch nicht nach weil der österreichische Gesetzgeber auch zur Umsetzung der RL verpflichtet ist wenn er wegen des fehlenden Spielraumes die Verletzung von Grundrechten begehen muss, sofern dies nicht die Grundprinzipien der Verfassung berührt, an diese nicht gebunden. Das so erlassene Gesetz ist demnach nicht als verfassungswidrig zu beurteilen.¹⁹¹ Überdies besteht der Anwendervorrang des Gemeinschaftsrechts auch gegenüber österreichischem Verfassungsrecht, sodass dieses auch anzuwenden ist, wenn seine Regelungen innerstaatlichen Grundrechten widersprechen.¹⁹² Das EU Sekundärrecht verlangt von den Mitgliedstaaten geeignete Maßregeln für die Durchsetzung der Offenlegung von Jahresabschlüssen. Eine geeignete Maßregel liegt nach der Rechtsprechung des EuGH nur vor, wenn sie wirksam, verhältnismäßig und abschreckend ist.¹⁹³

Nach überwiegender Auffassung wurden die Vorgaben der Richtlinie in Österreich ordnungsgemäß umgesetzt und entsprechen den gemeinschaftsrechtlichen Vorgaben. Im Hinblick auf die Umsetzungsverpflichtung des österreichischen Gesetzgebers und auf die Rechtsprechung des EuGH, unterliegen die maßgeblichen Bestimmungen des HGB (nun UGB) nicht einer innerstaatlichen Kontrolle durch den VfGH.

Bereits im Oktober 1999 hat der VfGH einen derartigen Individualantrag nach Art 140 B-VG auf Aufhebung der §§ 280, 283 HGB zurückgewiesen.¹⁹⁴ Eine verhängte Zwangsstrafe könne mittels Rechtsmittel oder Beschwerde an den VfGH bekämpft werden, aber für einen Antrag nach Art 140 B-VG fehle es an der unmittelbaren Betroffenheit des Antragstellers. (in diesem

¹⁹⁰ Gruber, wbl 2000, 251 (253) derselbe, Bilanzpublizität primär- und grundrechtskonform, wbl 2005, 161

¹⁹¹ Berka (FN 36), Rz 332; Mayer, Die österreichische Grundrechtsordnung nach dem EU-Beitritt, AnwBl 1996, 152 ff [157]

¹⁹² Thun-Hohenstein/Cede, Europarecht 88 f; OGH 29.3.2000 6 Ob 77/00t; OGH 9.3.2000 6 Ob 14/00b

¹⁹³ Gruber, RdW 1998, 525 (526)

¹⁹⁴ VfGH 5.10.1999 G 60/99; ebenso VfGH, ZfVB 2004/1193

Fall der Vorstand einer AG)¹⁹⁵ Ein Beschluss des EuGH in einer deutschen Vorabentscheidung vom September 2004, bestätigte schließlich indirekt die Auffassung sowohl des OGH als auch des VfGH bezüglich der Rechtmäßigkeit der Bilanzpublizität.¹⁹⁶

Auch eine gegenüber allen Geschäftsführern einer Gesellschaft ausgesprochene Zwangsstrafe (wegen der Nichtoffenlegung) führt nicht zu einer nicht zu rechtfertigenden Ungleichbehandlung gegenüber anderen Gesellschaften mit nur einem vertretungsbefugten Organ. Nach hL und Rsp wirkt sich eine unter mehreren Geschäftsführern vorgenommene Geschäftsverteilung nur im Innenverhältnis auf die Verantwortlichkeit der einzelnen Organe aus, und kann diese nicht von zwingenden gesetzlichen Verpflichtungen befreien.¹⁹⁷ Eine Ungleichbehandlung liegt bei Kapitalgesellschaften (AG, GmbH) im Vergleich zu Personengesellschaften auch nicht vor, da der Haftungsfond bei ersteren nur das Gesellschaftsvermögen umfasst während bei Personengesellschaften der persönlich haftende Gesellschafter mit seinem gesamten Vermögen für Verbindlichkeiten der Gesellschaft haftet. Es ist daher sachlich gerechtfertigt, dass Kapitalgesellschaften in der Frage der Offenlegung nicht gleich den Personengesellschaften behandelt werden.

In Bezug auf die Geheimhaltung personenbezogener Daten sieht Art 8 Abs 2 EMRK die Einschränkung dieses Grundrechts zum Schutz der Rechte und Freiheiten anderer, wie auch zur Wahrung berechtigter Interessen eines anderen wobei hier die Gegeninteressen abgewogen werden müssen. Da genau die Offenlegungspflicht ausschließlich dem Schutz Dritter (vor allem Gläubiger oder Vertragspartner) aus dem Grundgedanken des Gläubigerschutzes gilt, ist eine Einschränkung erlaubt und geboten.

Auch eine diesbezüglich Argumentation in Bezug auf § 5 Abs 3 Unternehmensreorganisationsgesetz (URG)¹⁹⁸ welches ausdrücklich eine Veröffentlichung dieses Verfahrens ausschließt, löste keine verfassungsrechtlichen Bedenken beim OGH aus.¹⁹⁹ Das URG bietet (noch) solventen, aber gefährdeten Unternehmen die Möglichkeit durch Reorganisationsmaßnahmen eine Verbesserung der Vermögens-, Finanz- und Ertragslage herbeizuführen (§ 1 URG) obwohl diese zur Einleitung nicht verpflichtet sind. § 1

¹⁹⁵ Zu der Tatbestandsvoraussetzung des Art 140 B-VG umfassend *Barfuß*, ÖJZ 1984, 533

¹⁹⁶ EuGH 23.9.2004, verb Rs C-435/02 und C-103/03, *Axel Springer AG/Zeitungsvorlag Niederrhein GmbH & Co Essen KG und Hans-Jürgen Weske*, EWS 2004, 510

¹⁹⁷ OGH 23.03.1993 2 Ob 526/93=SZ 66/40=ZVR 1994/29 S 77; RS0023825; *Koppensteiner*, GmbHG2 Rz 12 zu § 21; *Zehetner*, Folgen der Nichtoffenlegung des Jahresabschlusses, *ecolex* 1998, 482 ff

¹⁹⁸ § 5 Abs 3 URG lautet: (3) *Der Beschluss auf Einleitung des Reorganisationsverfahrens ist dem Unternehmer und dem Reorganisationsprüfer zuzustellen. Die Einleitung des Verfahrens ist nicht öffentlich bekanntzumachen.*

¹⁹⁹ OGH 28.6.2000, 6 Ob 162/00t

URG hat nach den Erläut der RV keinen Schutzgesetzcharakter.²⁰⁰ Ein damit verbundener Gläubigerschutz kann durch die Nichtveröffentlichung gegenüber Dritten aber nicht ausgeschaltet werden sondern wird, eigentlich ganz im Gegenteil, jetzt richtig schlagend, da Gläubiger über die hinterlegte Bilanz/Jahresabschluss erst jetzt von der Bestandsgefährdung des Unternehmens Kenntnis erlangen.

Eine diesbezügliche Zwangsstrafe bei Nichtbeachtung der Hinterlegungspflicht iSd § 283 UGB ist daher gerechtfertigt. Auch wenn die Zwangsstrafe wegen fortgesetzter Nichteinhaltung der gesetzlichen Verpflichtungen mehrmals gegen die Geschäftsführer verhängt wird, ist dies nicht unverhältnismäßig. Die Offenlegungspflicht des Jahresabschlusses ist daher EU- und grundrechtskonform.²⁰¹

²⁰⁰ MSA, URG Anm 3 zu § 1

²⁰¹ OGH 15.12.1999, 6 Ob307/99m, RdW 2000/250, 283

3.4. Die „Offenlegungspflichten“ von Auskunftfeien

Bisher galt es als strenges Geschäftsgeheimnis woher Auskunftfeien ihre Informationen für eine Bonitätsbeurteilung bezogen. Ein Auskunftsbegehren nach § 26 DSG wurde meistens nur ungenau und sehr wage beantwortet. Jedoch wurde durch zwei Entscheidungen des VwGH²⁰² dieser Praxis nun „ein Riegel vorgeschoben“ da grundsätzlich jeder das Recht hat, schriftlich von jedem Auftraggeber eine Datenverarbeitung, Auskunft über ihn betreffende personenbezogenen Daten zu verlangen. Dies hat aufgrund § 26 Abs 6 DSG 2000 einmal pro Jahr und Aufgabengebiet kostenlos zu erfolgen. (siehe dazu auch Kapitel 14.1.)

In dem oben angeführten Urteil wird die Auskunftfei (in diesem Fall der Kreditschutzverband) nun beauftragt, auch die Herkunft der Daten im Detail zu nennen. Dies wurde mit dem Argument versucht zu verhindern, dass wenn er bekannt geben müsste von wem konkret die Auskünfte über die Zahlungsfähigkeit von Schuldner kämen, die seine Geschäftstätigkeit andernfalls unmöglich mache. Die von ihm genannten allgemeinen Bezeichnungen wie „Banken und Lieferanten“ wurden weder von der Datenschutzkommission (DSK) noch vom VwGH all ausreichend angesehen. Damit der Betroffene sein Recht auf Richtigstellung etwaiger falscher Daten durchsetzen kann, muss ihm der Name und Adresse des Datenlieferanten bekannt gegeben werden. Gleichzeitig muss jedoch auch erwähnt werden, dass es sich um das Auskunftsrecht um kein absolutes Recht handelt sondern dieses seine Grenzen in berechtigten Interesse des Auftraggebers oder Dritter sofern in einer konkreten Situation diese als „überwiegend“ zu werten sind. Der KSV argumentierte, dass die Daten betriebsinterne Bereiche beträfen, Interessen der Datenquellen beeinträchtigten und überdies Betriebsgeheimnisse seien. Der Auskunftswerber müsse daher besondere Gründe nennen, um nähere Informationen zu erhalten. Nach Ansicht des VwGH wurde dem Auskunftsbegehren ausreichend Genüge getan, wenn hinsichtlich jeder Datenart, die konkrete Quelle angegeben wird. Diese Quelle sei noch kein Betriebsgeheimnis und somit seien keine überwiegenden Interessen an der Geheimhaltung der Herkunft der Daten gegeben und entschieden daher zu Gunsten des Auskunftswerbers. Zu betonen ist, dass der Auskunftswerber nicht danach fragte, WAS die Banken und Lieferanten dem KSV mitgeteilt haben da es sich hiebei wohl um ein schützenswertes Betriebsgeheimnis handeln dürfte.²⁰³

²⁰² VwGH 23.1.2007 2006/06/0039 und VwGH 19.12.2006 2005/06/0111

²⁰³ Die Presse 19.3. und 26.3.2007

Andererseits kann und darf sich niemand nur auf die Bonitätsinformationen der Kreditauskunfteien verlassen. Obwohl der OGH in der Entscheidung 2 Ob 36/28²⁰⁴ eine Nachforschungspflicht (in diesem Fall eine Krankenkasse) aufgrund von Zeitungsberichten verneint hat, ist er mit der Entscheidung OGH 6 Ob 192/03h²⁰⁵ von dieser Rechtsansicht abgewichen und verlangt nun in stRsp auch den aktiven Beitrag der Nachforschungspflicht von Gläubigerseite. So ist die Einrichtung eines „Überwachungssystems“ und die Überprüfung der Tagespresse für ein mittelgroßes Unternehmen grundsätzlich zumutbar und eine Unterlassung eines solchen Systems als fahrlässig zu qualifizieren. Leichte Fahrlässigkeit reicht dabei aus. Ob eine leichte Fahrlässigkeit vorliegt, bestimmt sich nach der zum Zeitpunkt der Rechtshandlungen zur Verfügung stehenden Informationen, die zumutbarer Weise herangezogen werden können und ihrer ordnungsgemäßen Auswertung.²⁰⁶ Die Ignorierung von übereinstimmenden Presseberichten mit entsprechenden Sachverhaltssubstrat ist sorgfaltswidrig und gilt auch für Gläubigergruppen die schon bisher einem strengen Sorgfaltsmaßstab unterworfen sind wie Banken und Finanzämter im allgemeinen und die „Hausbank“ im besonderen weil diese aufgrund der Bonitätsprüfung und –überwachung über ein größeres Maß an Beurteilungsfähigkeit und eine entsprechende sachliche und personelle Organisation verfügen.²⁰⁷ Der OGH greift eine Entscheidung des deutschen BGH auf ()²⁰⁸ wonach Zeitungsmeldungen nicht unmittelbar eine Zahlungsunfähigkeit bedeuten jedoch in der Regel eine „Erkundigungspflicht“ begründen wenn der oder die gleich lautenden Zeitungsartikel inhaltlich substantiiert erscheinen und einen Gläubiger veranlassen müssten, Erkundigungen über die Zahlungsfähigkeit eines Schuldners einzuholen. Erkundigungen können über eine Kreditauskunftei/Gläubigerschutzverband, beim Firmenbuchgericht durch Einsicht in die Jahresabschlüsse oder auch direkt beim Gläubiger erfolgen.

In diesem Falle handelte es sich um Anfechtung nach der KO iSd §§ 28 Z 1 und 2, 30 Abs 1 Z 2 und 3 sowie 31 Abs 1 Z 2 jedoch zeigt diese Entscheidung allgemein, dass ein internes Bonitätsprüfungssystem (ab einer mittleren Unternehmensgröße) für auch bereits bestehende Geschäftsverbindungen unerlässlich ist und finanzielle Risiken aufgrund eigener Nachforschungen wenn schon nicht ausgeschalten aber doch zu mindestens verringert bzw. minimiert werden können.

²⁰⁴ JBl 1928, 323

²⁰⁵ ZIK 1/2004, Artikel Nr. 25, 24

²⁰⁶ OGH 28.9.2000 8 Ob 37/00z

²⁰⁷ SZ 73/182 mwN; OGH 26.4.2001 6 Ob 37/01m; König, die Anfechtung nach der Konkursordnung, 3. Aufl., Rz 11/24; Weissel, ÖBA 1994, 955

²⁰⁸ BGH ZIP 2001, 1641 kommentiert von Pappe, EWiR 2001, 959

4. Wirtschaftliche Aspekte

Im Jahr 2007 wurden bei den 3500 Bankomaten und 7600 Bargeldautomaten 133,6 Mio Transaktionen mit einem Volumen von € 17,7 Mrd. getätigt was einer Umsatzsteigerung von 8 % sowie einer 9,2 %igen Transaktionssteigerung gegenüber 2006 entspricht.²⁰⁹ Die österreichischen Privathaushalte schulden den Banken € 116,3 Mrd, die österreichischen Unternehmen € 129,5 Mrd.

Ca. 150.000 Menschen gelten in Österreich als zahlungsunfähig. 300.000 Österreicher haben Probleme ihre Rechnungen zu bezahlen bzw. sind überschuldungsgefährdet.

2003: Durchschnittl. Meridian Verschuldung € 37.200,--

(= 50 % haben mehr Schulden, 50 % haben weniger)

2004: Durchschnittl. Meridian Verschuldung € 35.800,--²¹⁰

Schuldenreport 2006 (f. 2005):

- Durchschnitt. Meridian Verschuldung € 38.800,--
- Durchschnittverschuldung gesamt: € 74.483,--
- 6694 Konkursanträge, 5520 KO
- 961.557 Fahrnisexekution
- 775.562 Forderungsexekutionen

Schuldenreport 2007 (f. 2006)

Durchschnitt. Meridian Verschuldung € 38.038,--

Durchschnittverschuldung gesamt € 75.357,--

- 7509 Konkursanträge, 6296 Konkurseröffnungen
- 943.249 Fahrnisexekutionen
- 762.105 Forderungsexekutionen

Schuldenreport 2008 (f. 2007)

Die durchschnittliche (Meridian-) Verschuldung € 39.800,--.

Durchschnittverschuldung gesamt € 76.407,--

- 8717 Konkursanträge, 7.388 Konkurseröffnungen,
- 930.787 Fahrnisexekutionen

²⁰⁹ Economy, No. 54, 32

²¹⁰ Für diese beiden Jahre und davor gibt es leider keine genaueren Zahlen

- 760.200 Forderungsexekutionen

Aktuelle Zahlen für 2008 (3. Quartal)

- 7.271 Konkursanträge, 6469 Konkursöffnungen

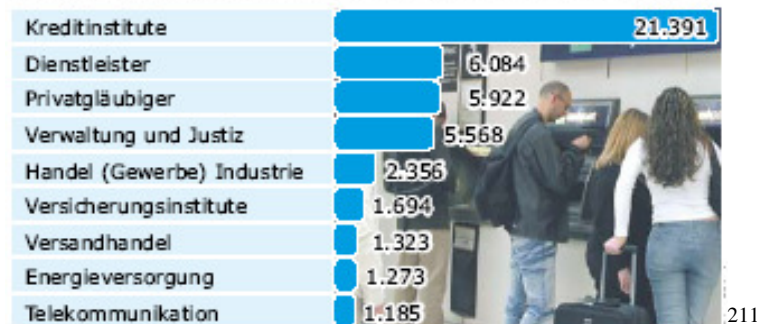
Auf das Jahr 2008 hochgerechnet wird mit ca. 8550 Konkursöffnungen gerechnet (+17 %)

Für 2007 ergibt sich folgende durchschnittliche Schuldenaufstellung:

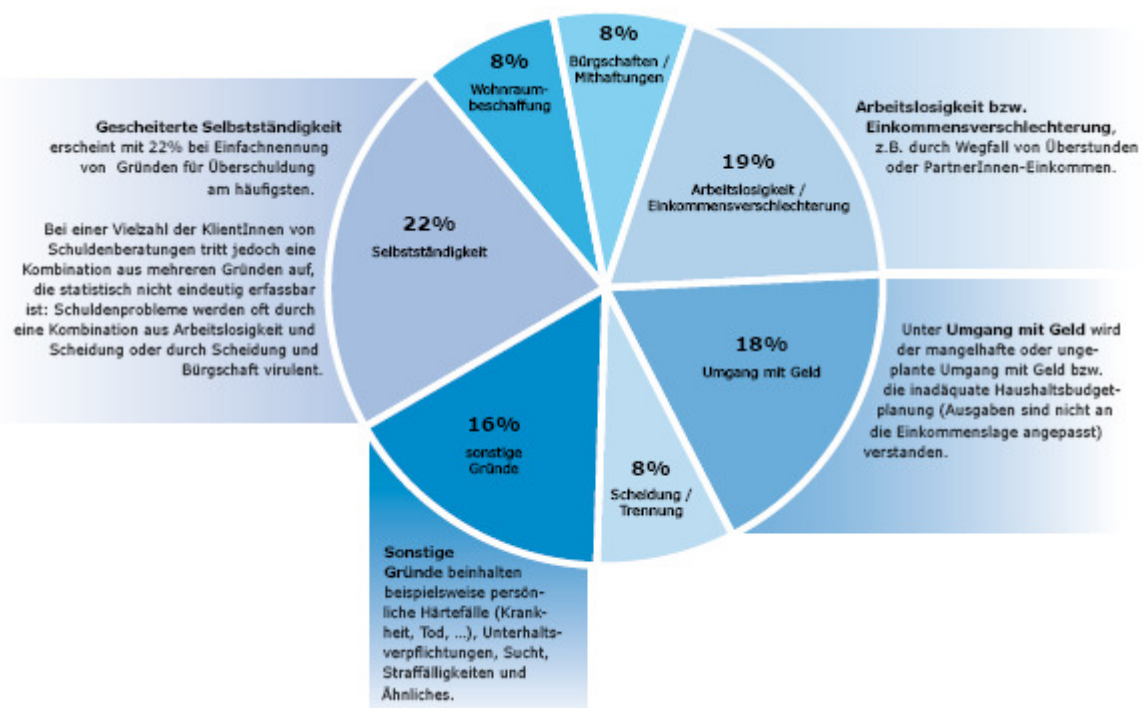
Höhe der Schulden nach Gläubiger

Durchschnittliche Verschuldung in Euro

Die durchschnittliche Höhe der Schulden steigt jährlich leicht an, ein Großteil der KlientInnen steht mit maximal 50.000 Euro in der Kreide.
Eine interessante Aufstellung ist auch die **Schuldenshöhe nach Gläubigern**. Hier zeigt sich, dass die Gruppe der Kreditinstitute und Banken den höchsten Durchschnittswert an Forderungen gegenüber KlientInnen der Schuldenberatungen hat. Damit sind die Banken seit Jahren Spitzenreiter als Gläubiger – Tendenz steigend.



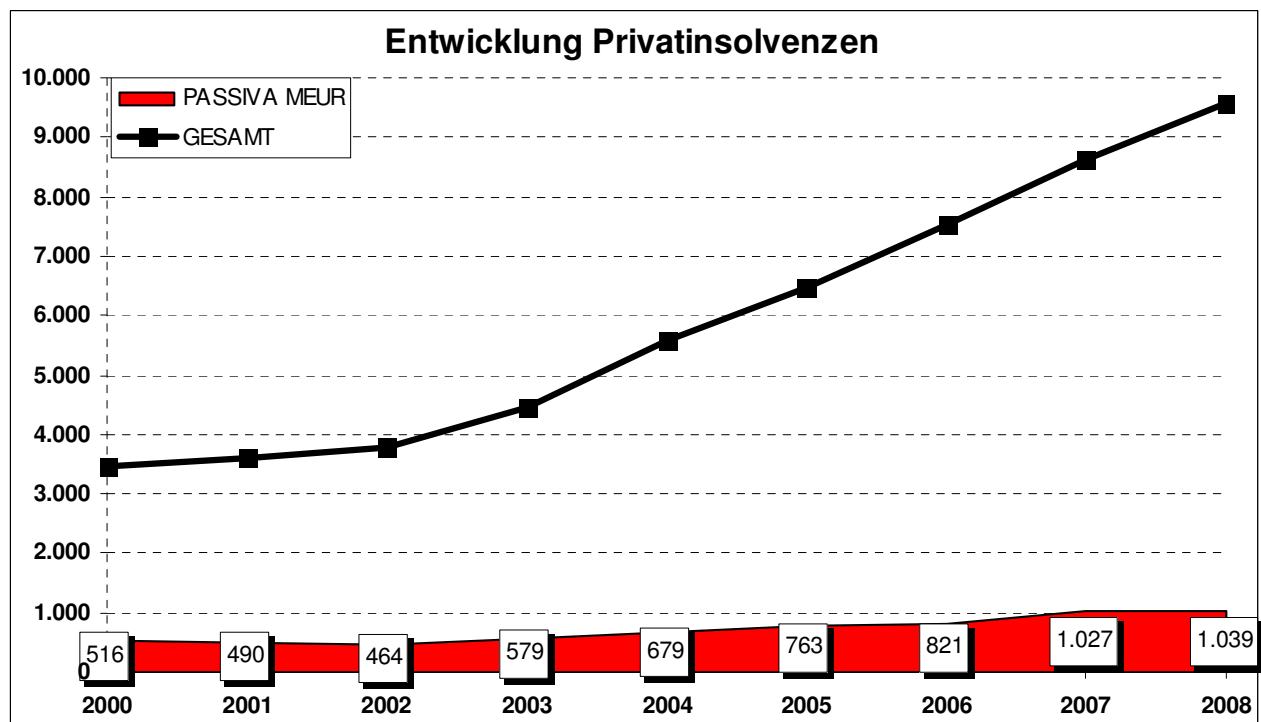
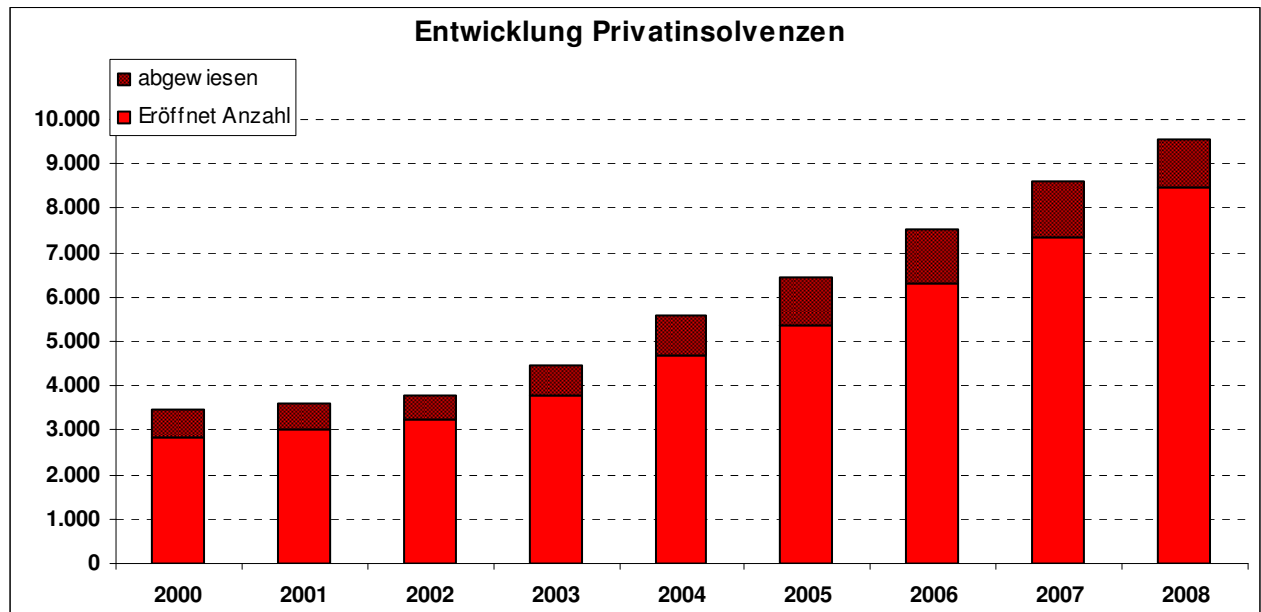
GRÜNDE FÜR DIE ÜBERSCHULDUNG (Einfachbenennungen und Erstberatungen 2007)²¹²



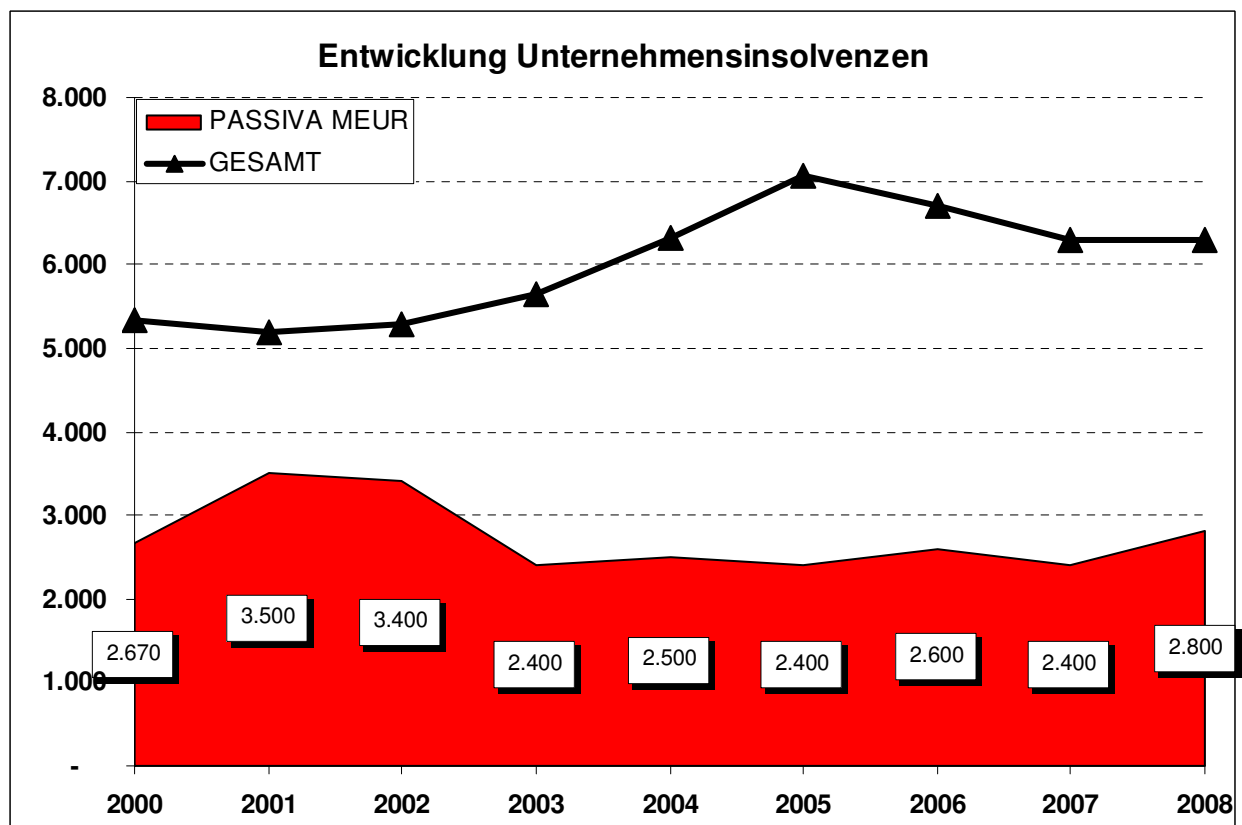
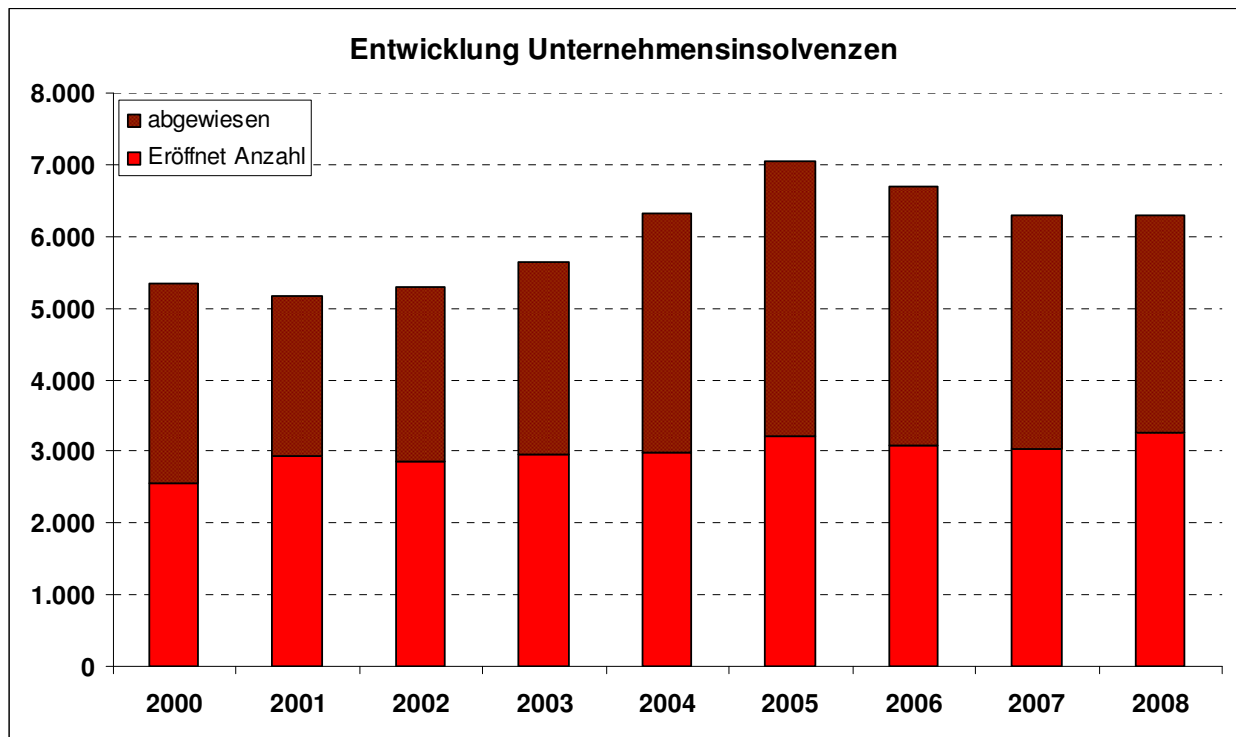
²¹¹ Quelle: Schuldenreport 2008

²¹² Siehe FN 211

Insolvenzentwicklung Privatpersonen:



Insolvenzentwicklung Unternehmen:



5. Die Prüfung der Zulässigkeit der Datenermittlung

Zuerst ist die Frage zu lösen ob überhaupt eine dem DSG unterliegende Datenverarbeitung vorliegt ?

1. Liegt eine maschinelle und programmgesteuerte Datenverarbeitung vor ?
2. Werden im Rahmen dieser Datenverarbeitung personenbezogene Daten verarbeitet oder etwa nur technische Daten für die Produktion ?
3. Ist die Selektierbarkeit nach mindestens einem Kriterium gegeben ?

Wenn danach diese Frage bejaht werden kann und das DSG zur Anwendung kommt, ist die Zulässigkeit der Ermittlung und Verarbeitung zu prüfen. Vorerst ist jedoch die Meldepflicht des Auftraggebers iSd § 17 DSG 2000 zu beachten welcher besagt, dass vor Aufnahme einer Datenanwendung eine Meldung an die DSK zum Zwecke der Registrierung im DVR zu erstatten ist.

Die Ausnahmen in § 17 Abs 2 (und Abs 3 welcher sich mit staatsbezogenen Aufgaben befasst) DSG 2000 befreien von der Meldepflicht in folgenden Fällen:

- Veröffentlichte Daten, dh jedermann kann persönliche Daten aus Telefonbüchern, aus der Zeitung, dem Internet²¹³ verarbeiten
- Daten, um damit ein öffentliches Register zu führen, zB Melderegister, Firmenbuch, Grundbuch (siehe aber Ausnahme Kapitel I, Seite 7, FN 17)
- Anonyme Daten (=Angaben die niemand auf eine Person zurückführen kann)
- Daten für persönliche oder familiäre Zwecke durch Privatpersonen
- Daten für publizistische Zwecke iSd § 48 DSG 2000
- Daten die unter eine Standardanwendung fallen

Auch das DSG 2000 geht grundsätzlich vom Verbotsprinzip aus, dh dass die Ermittlung und automationsunterstützte Verarbeitung personenbezogener Daten grundsätzlich verboten ist, falls nicht ein berechtigter Zweck des privaten Rechtsträgers nachgewiesen werden kann und schutzwürdige Interesse des Betroffenen geachtet werden. Die DS-RL sieht ein zweistufiges Zulässigkeitskonzept für die Verarbeitung von personenbezogenen Daten vor. Nach Art 6 DS-

²¹³ *Drobesch/Grosinger*, Datenschutzgesetz, 144

RL muss die Verarbeitung zuerst eine Reihe von spezifischen Kriterien erfüllen, um zulässig zu sein.²¹⁴

Im ersten Schritt sind die allgemeinen Voraussetzungen des § 6 DSG 2000 (welcher im Großen und Ganzen Art 6 DS-RL entspricht) zu prüfen. Diese gelten unterschiedslos für alle Arten der Datenverwendung.

5.1. Der Begriff von „Treu und Glauben“

Es wurde hier der bis dato der österreichischen Rechtsordnung unbekannte Begriff von „*Treu und Glauben*“ aufgenommen. (§ 6 Abs 1 Z 1 DSG 2000) Die Definition dieses Begriffes bereitet Schwierigkeiten²¹⁵. Zur näheren Festlegung, was in den einzelnen Bereichen als Verwendung von Daten nach „Treu und Glauben“ anzusehen ist, können gemäß § 6 Abs 4 DSG 2000 für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen, Verhaltensregeln ausarbeiten, welche jedoch einer Begutachtung durch den Bundeskanzler benötigen.²¹⁶ Dies führt natürlich gleich zur Frage der rechtlichen Qualität dieser „Verhaltensregeln bzw. „*codes of conduct*“. Sollten sie zB als Satzung Verordnungscharakter haben, könnte ein allfälliger Widerspruch zum DSG vor dem VfGH als gesetzwidrig bekämpft werden. Wenn diese jedoch nur unverbindlichen Charakter besitzen, käme ihnen nur die Definition einer Empfehlung zu welche jedoch wiederum nicht anfechtbar wäre.²¹⁷

²¹⁴ Art 6 Datenschutz RL sieht vor, dass personenbezogenen Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden ;für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen; den Zwecken entsprechen, für die sie erhoben und/oder weiterarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen; sachlich richtig und, wenn nötig, auf dem neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden nicht länger, als für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen

²¹⁵ Dammann/Simits, EG DS-RL, verstehen darunter eine Auffangklausel, um unklare Rechtsgrundlagen einer Datenverwendung negativ beurteilen zu können; Ehmann/Helfrich, EG DS-RL, Kurzkommentar (1999) 111, verweisen auf die nationalen Normgeber und Rechtssprechung; Henke, Die Datenschutzkonvention des Europarates (1986) 101, versteht darunter neben der Rechtmäßigkeit die Transparenz der Datenverwendung gegenüber dem Betroffenen. Auch die ErläutRV 1613 BlgNR XX. GP verweisen auf den 4. Abschnitt des DSG 2000 betreffend die Publizität der Datenverarbeitungen

²¹⁶ zB Direct Marketing Verband Österreich gemeinsam mit der Wirtschaftskammer Österreich
<http://www.dmvoe.at/services/die-branche/ressorts/data-studien-recht/fair-data-code-of-conducts.html>

²¹⁷ Mayer-Schönberger/Brandl, DSG 2000², 26 halten die Heranziehung von ÖNORMEN für möglich. ÖNORMEN haben auf Grund der Bewilligung durch die Aufsichtsbehörde bindenden Charakter (Selbstbindung der Verwaltung)

Andere wiederum sehen im § 69 Abs 2 GewO²¹⁸ betreffend die Ausübungsregeln für Gewerbebetriebe welche ausdrücklich auch dem Schutz der Privatsphäre dienen, ein Mittel diesen im Sinne des § 6 Abs 4 DSG 2000 nutzbar zu machen.²¹⁹ Ein Verstoß gegen den Grundsatz von „Treu und Glauben“ wäre zB das heimliche Sammeln von Daten²²⁰, die Täuschung des Betroffenen über den Zweck der Datenanwendung oder über ihm zustehende Rechte wie das Recht auf Auskunft, Richtigstellung, Löschung und Widerspruch, sofern sich nicht schon aus den ausdrücklich normierten Informationspflichten und Auskunftsrechten bereits eine Rechtswidrigkeit ergibt. Allgemein kann festgehalten werden, dass dieser Grundsatz vor allem die Funktion eines Auffangtatbestandes der letztlich vom Auftraggeber rechtmäßiges Verhalten verlangt. Wenn nun eine eindeutige Regelung über die Zulässigkeit einer bestimmten Datenverwendung fehlt, wird man diese ggf unter Berufung auf § 6 Abs 1 Z 1 DSG 2000 als rechtswidrig qualifizieren können.²²¹

*Duschanek/Rosenmayr-Klemenz*²²² verstehen unter der Datenverwendung nach „Treu und Glauben“ bzw. „auf rechtmäßige Weise“ nur den Hinweis auf die Einhaltung der Bestimmungen des DSG bzw. gegebenenfalls weiterer bereichsspezifischer Bestimmungen.

²¹⁸ § 69 Abs 2 GewO lautet: *Der Bundesminister für wirtschaftliche Angelegenheiten hat im Einvernehmen mit dem Bundesminister für Gesundheit, Sport und Konsumentenschutz durch Verordnung festzulegen, welche Maßnahmen die Gewerbetreibenden bei der Gewerbeausübung hinsichtlich der Einrichtung der Betriebsstätten, hinsichtlich der Waren, die sie erzeugen, verkaufen oder vermieten oder deren Verkauf sie vermitteln, hinsichtlich der Einrichtungen oder sonstigen Gegenstände, die sie zur Benützung bereithalten, oder hinsichtlich der Dienstleistungen, die sie erbringen, zu treffen haben, soweit dies zum Schutz der Interessen der von der Gewerbeausübung betroffenen Personen, insbesondere zum Schutz vor Vermögensschäden oder vor Belästigung wie etwa durch Eindringen in die Privatsphäre, erforderlich ist (Ausübungsregeln). Bei der Erlassung solcher Verordnungen ist insbesondere auch auf die Beobachtungen und Berichte von Konsumentenberatungseinrichtungen sowie auf die Berichte des Bundesministers für Gesundheit, Sport und Konsumentenschutz über die Lage der Verbraucher Bedacht zu nehmen. Weiters kann der Bundesminister für wirtschaftliche Angelegenheiten nach Anhörung der zuständigen Gliederung der Bundeskammer der gewerblichen Wirtschaft durch Verordnung Regeln über die Verhaltensweisen, die bei der Ausübung eines bestimmten Gewerbes einzuhalten sind, und über die für die Gewerbeausübung erforderliche Betriebsausstattung festlegen (Standesregeln); hiebei ist auf die Gewohnheiten und Gebräuche, die in diesem Gewerbe von Personen, die die Sorgfalt eines ordentlichen Kaufmannes anwenden, eingehalten werden und auf die Anforderungen, die von den die Leistungen dieses Gewerbes in Anspruch nehmenden Personen üblicherweise gestellt werden, sowie darauf Bedacht zu nehmen, dass das Ansehen des betreffenden Gewerbes und das Vertrauen aller von der Gewerbeausübung berührten Personen in die das Gewerbe ausübenden Gewerbetreibenden gewahrt bleibt; soweit dabei der Schutz des Vertrauens der von der Gewerbeausübung betroffenen Personen im Vordergrund steht, insbesondere hinsichtlich der Festlegung von Höchstbeträgen im Sinne der Z 5, ist hiebei das Einvernehmen mit dem Bundesminister für Gesundheit und Konsumentenschutz herzustellen. Verordnungen über Standesregeln können zum Gegenstand haben zum Beispiel Bestimmungen über*

1. das standesgemäße Verhalten im Geschäftsverkehr mit den Auftraggebern,
2. das standesgemäße Verhalten gegenüber anderen Berufsangehörigen oder Angehörigen anderer Berufe, die durch die Gewerbeausübung berührt werden,
3. das standesgemäße Verhalten gegenüber Personen, die weder Auftraggeber noch Berufsangehörige sind, auf die sich aber die Gewerbeausübung bezieht oder die von der Gewerbeausübung betroffen sind,
4. die Ausstattung des Betriebes, die eine standesgemäße Berufsausübung gewährleistet,
5. für das Gewerbe der Arbeitsvermittlung (§ 94 Z 1), der Immobilienmakler (§ 94 Z 35), der Immobilienverwalter (§ 94 Z 35), der Inkassoinstitute (§ 94 Z 36) und der Personalkreditvermittler (§ 94 Z 75) die Höchstbeträge der den Gewerbetreibenden gebührenden Provisionssätze oder sonstigen Vergütungen.

²¹⁹ *Duschanek*, Neuerungen und offene Fragen im DSG 2000, ZfV 2000/1303, 530

²²⁰ OGH 15.12.2006, 6 Ob 275/05t=EvBl 2006/66=ÖJZ-LSK 2006/84.

²²¹ *Grabenwarter*, ÖJZ 2000, 864; *Dammann/Simitis*, EG DS-RL, 139 unter Hinweis auf die Begründung zur RL

²²² Vgl hiezu *Duschanek/Rosenmayr-Klemenz*, DSG, § 6 Komm2; aA wohl *Dohr/Pollirer/Weiss*, DSG², § 6 Anm 4 u 5

5.2. Der anerkannte Zweck

Auch will der Gesetzgeber die Ermittlung und Verarbeitung von personenbezogenen Daten durch Private auf den von der gültigen Rechtsordnung anerkannten Zweck des privaten Rechtsträger abstellen. (§ 6 Abs 1 Z 2 und 3 DSG 2000) Im Zentrum der Zulässigkeitsprüfung steht die strikte Zweckbindung. Der Zweck muss festgelegt, eindeutig und rechtmäßig sein²²³ und eine spätere Änderung des Zwecks ist unzulässig. Der Zweck muss so klar zum Ausdruck gebracht werden, dass Zweifel daran, ob und in welchem Sinn der Auftraggeber den Zweck festgelegt hat, ausgeschlossen sind. Die Daten müssen für den Zweck erheblich sein und dürfen im Umfang nicht über den Zweck hinausgehen.²²⁴ Vorsorglich angelegte Datensammlungen ohne konkret definierte und rechtmäßige Funktion sind daher unzulässig.²²⁵

In der Regel wird sich ein solcher zB aus dem Gesetz, aus dem Firmenbuch in Verbindung mit dem Gesellschaftsvertrag, aufgrund der Gewerbeberechtigung nach § 152 GewO oder bei Vereinen aus den Vereinsstatuten ableiten lassen.²²⁶ Diese Forderung die vor allem aus den USA vor dem „Fair Credit Reporting Act“ (1970) eine bedeutende Rolle spielte, ist dahin zu verstehen, dass man sich bei der Ermittlung von Daten nicht dubioser Quellen, zweifelhafter Beschaffungsmethoden (zB Befragung von Kontaktpersonen, Auswertung von Klatschkolumnen in der Presse) bedient, sondern dem Kontakt mit dem Betroffenen und der Überprüfbarkeit des Gehaltes der Information mehr Augenmerk schenken soll.

In Bezug auf welche Daten nun für den festgestellten Unternehmenszweck notwendig sind oder wenigstens mit ihm zusammenhängen, ergibt sich aufgrund der Rechtsordnung aus der Zuordnung der unterschiedlichen Unternehmenstätigkeiten in verschiedene Kategorien und dadurch die grundsätzliche Unzulässigkeit von Datenverarbeitungen für Unternehmen die einer anderen Sparte zuzurechnen wären und deren Geschäftszweck nicht zu dieser Sparte gehört. Aus dem konkreten Unternehmenszweck ergibt sich nun die Zulässigkeit der einzelnen Datenarten für das Unternehmen, wobei der konkrete Unternehmenszweck vor allem für die Zulässigkeit von Daten über Lieferanten, über Kunden und potentielle Kunden entscheidend ist. Die im einzelnen zulässigen Daten werden sich aus der bereits erwähnten

²²³ Art 6 Abs 1 lit b DS-RL

²²⁴ Art 6 Abs 1 lit c DS-RL

²²⁵ *Dammann/Simitis*; EG DS-RL, 79

²²⁶ *Weiss/Pollirer*, RWZ 1993/4, Datenschutz in der Wirtschaft, 114

Berechtigung des Unternehmens *und* aus dem mit diesem Kunden bestehenden individuellen Vertragsverhältnis ergeben. (uU auch die Zulässigkeit der Verarbeitung von personenbezogenen Daten die mit diesem Vertrag in Zusammenhang stehen zB Bürgen bei einem Kredit, Empfänger einer Überweisung). Ferner sind Tätigkeiten, die weder im DSGVO noch im Unternehmensgegenstand, noch im Gewerbeschein, noch im Gesetz gesondert Erwähnung finden, aber für die Entfaltung gewerblicher Tätigkeit erforderlich sind, vom Zweck auch eines gewerblich tätigen Unternehmens gedeckt (Beschaffung von Material, Beschäftigung von Arbeitskräften etc).²²⁷

Man kann für die Detailbeurteilung der Zulässigkeit eine Reihung aufstellen, die eine Einteilung von Daten nach ihrem Naheverhältnis zum Privat- und Familienleben des Betroffenen versucht:

1. Name, Adresse, Geburtsdatum, Telefonnummer
2. Informationen aus öffentlich zugänglichen Quellen; berufliche Stellung, Ausbildung
3. Finanzielle Stellung, Einkommen, Bonität, finanzielle Verpflichtungen
4. Freizeitgewohnheiten, Liebhabereien, Lebensgewohnheiten, Kaufgewohnheiten
5. Verdachtsmomente, Vorstrafen (Leumund), Intimleben, Daten der Psyche, Familiendaten, Krankheiten

Die Vermutung der Zulässigkeit wird oben nach unten abnehmen und sich in den unteren (inneren) Bereichen in der Vermutung der Unzulässigkeit umkehren, die nur durch die Notwendigkeit für einen bestimmten Unternehmenszweck widerlegt werden kann.²²⁸

In wenigen Fällen ergibt sich aus der Rechtsordnung bereits eine eindeutige Aussage über die Unzulässigkeit einzelner Datenarten (zB nach § 152 Abs 1 für Kreditauskunfteien für – andere – private Verhältnisse) welche jedoch in den Auskünften mit „blumigen Formulierungen“ oder mit dem Vermerk der telefonischen Bekanntgabe elegant umgangen werden.

²²⁷ Grabenwarter, ÖJZ 2000, 866

²²⁸ zB die Speicherung von Krankengeschichten nach § 10 KAKuG

5.3. Die sachliche Richtigkeit

Gemäß § 6 Abs 1 Z 4 müssen die zu verwendenden Daten „im Hinblick auf die den Verwendungszweck sachlich richtig“ und „wenn nötig auf dem neuesten Stand“ sein. dürfen nicht länger, als es für die Realisierung des Zwecks erforderlich ist, gespeichert werden.^{229 230}

Dies soll vor allem den Betroffenen als Schutz vor Nachteilen aufgrund unrichtiger oder nicht aktueller Daten dienen. Es wird dem Auftraggeber daher eine konkrete Handlungspflicht diesbezüglich auferlegt, die Daten zu prüfen und regelmäßig zu aktualisieren. Diese Pflicht wird sodann noch weiters in § 27 DSG 2000 („Recht auf Richtigstellung und Löschung“ – siehe Kapitel 14.2.) weiter konkretisiert.

Einen fix vorgegebenen Zeitintervall gibt es diesbezüglich nicht jedoch ergeben sich Anhaltspunkte dass das Gesetz von der Richtigkeit und Aktualität ausgeht. Bei Daten welche nie bis selten eine Änderung erfahren (zB das Geburtsdatum, Sozialversicherungsnummer, Familienstand,...) ist es sicherlich nicht nötig diese andauernd auf den neuesten Stand zu bringen. Auch kann eine regelmäßige Aktualisierung unterbleiben wo dem Betroffenen keine Nachteile aus überholten Daten erwachsen. (zB Adresse)²³¹

Hohe Anforderungen gelten dagegen für Datenverwendungen im Rahmen von Auskunfteien/Kreditevidenzen. Da eine fortwährende Aktualisierung und Richtigstellung aus wirtschaftlichen Gründen fast nicht möglich ist, wird jedem Ereignis ein bestimmtes Datum beigelegt und somit die Aktualität und Richtigkeit zum jeweiligen Zeitpunkt gewahrt.²³²

Wirtschaftsauskunfteien welche die Bonitätsdaten der von ihnen beauskunfteten Personen vor Erteilung der Auskunft über die Kreditwürdigkeit nicht auf sachliche (inhaltliche) Richtigkeit und Aktualität überprüfen, verletzen den Betroffenen in seinem Recht auf Geheimhaltung personenbezogener Daten. Im Falle einer konkreten Schädigung (zB Verweigerung eines Vertragsabschlusses aufgrund falscher Bonitätsauskunft) stellt die inhaltliche Unrichtigkeit als Verstoß gegen den Grundsatz auf sachliche Richtigkeit, eine Rechtswidrigkeit dar.²³³

5.4. Die Aufbewahrungsdauer

Der Auftraggeber wird weiters iSd § 6 Abs 1 Z 5 DSG 2000 zu untersuchen haben, ob alle Daten auch wirklich noch benötigt werden, etwa nach Ablauf gesetzlicher

²²⁹ Art 6 Abs 1 lit d und e DS-RL

²³⁰ Mayer-Schönberger-Zeiger-Kronegger, Auf dem Weg nach Europa: Zur Novellierung des DSG, ÖJZ 1998, 249

²³¹ Grabenwarter, ÖJZ 2001, 861; Siegwart in Jähnel (Hrsg), Aktuelle Fragen des Datenschutzrechts, 220

²³² Dammann/Simitis, EG DS-RL, 142; Duschaneck/Rosenmayr-Klemenz, DSG 2000, 40;

²³³ Trotzmüller, Die Durchsetzbarkeit des Rechts auf Datenschutz im Lichte der Judikatur, Diss Uni Wien, 53

Aufbewahrungspflichten, um den Geschäfts- oder Vereinszweck erfüllen zu können. Dieser ebenfalls mit der Zweckbestimmung verknüpften Anforderung liegt der Gedanke zugrunde dass Daten nur innerhalb einer bestimmten Zeitdauer welche aufgrund der Datenverwendung determiniert ist, aufbewahrt werden dürfen. Somit kann eine bis zu einem durch die Zweckbindung bestimmten Zeitpunkt rechtmäßige Datenverwendung nach Beendigung der Datenverarbeitung in eine unzulässige Datenverwendung umschlagen. Allerdings wird diese Rechtsfolge durch § 27 Abs 6 DSG 2000 hinausgeschoben, wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützten lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann. Zwischenzeitlich sind solche Daten bis zu einem solchen Zeitpunkt für den Zugriff zu sperren.²³⁴ Die Grenze liegt jedoch immer bei den schutzwürdigen Interessen des Betroffenen im Sinne der §§ 8 und 9 DSG. Zu beachten ist jedoch die Ausnahme in § 152 Abs 2 GewO für Kreditauskunfteien, das im Falle der Endigung der Gewerbeberechtigung der Schriftwechsel und die Geschäftsbücher zu vernichten sind, auch dann wenn der Zeitraum von sieben Jahren noch nicht verstrichen ist.

Erst in einem zweiten Schritt- in Art 7 DS-RL – folgen die konkreten Erlaubnistatbestände, die grob den §§ 6 und 17 DSG 2000 entsprechen, allerdings wesentlich detaillierter sind. Diese beiden Schritte dürfen nicht alternativ gesehen werden sondern müssen zusammen vom Verarbeiter gesetzt werden da erst wenn beide Kriterien – das der Zulässigkeitsvoraussetzungen und das der Erlaubnistatbestände – erfüllt sind, eine Verarbeitung legitim ist. Gerade beim Schritt der Zulässigkeitsprüfung versucht der europäische Gesetzgeber über die Facetten der Zweckbindung sicherzustellen, dass die jeweils richtigen Daten im jeweils passenden Kontext verarbeitet werden weil ansonsten bei Verlust des Konnex zwischen Daten und Kontext, der Betroffene im nachhinein seiner informationellen Selbstbestimmungs- und Partizipationsmöglichkeiten beraubt wird.²³⁵ Nur wenn sich die Bürger darauf verlassen können, dass ihr informationeller Wille auch zukünftig Beachtung findet, wird ihnen tatsächliche Selbstbestimmung zuteil. Die Zweckbindung der Datenverarbeitung ist das Mittel dazu.

Selbst bei einer grundsätzlichen Zulässigkeit der Datenverarbeitung kann sich im Einzelfall aus einer besonderen Problemstellung heraus wegen der zweiten Grenze der Zulässigkeit, die Beachtung schutzwürdiger Interessen des Betroffenen eine Unzulässigkeit im Einzelfall

²³⁴ Duschaneck/Rosenmayr-Klemenz, Datenschutzgesetz 2000, 40; Grabenwarter ÖJZ 2000, 866

²³⁵ Brühann/Zerdick, nennen dies „Doppelprüfung“; „zuerst müssen die Daten den Kriterien des Art 6 entsprechen. Diese solchermaßen beschaffenen Daten dürfen wiederum nur dann verarbeitet werden, wenn die Anforderungen des Art 7 oder 8 erfüllt sind“, Umsetzung, 558 sowie Dammann/Simitis ,EG DS-RL, 139

ergeben. Es ist unbestritten, dass die „Branchenüblichkeit“ der Verarbeitung bestimmter Datenarten ein Indiz für die Zulässigkeit ergibt aber diese wird immer an den schutzwürdigen Interessen des Betroffenen zu messen sein.²³⁶

Bei Nichtberechtigung gemäß § 7 DSG 2000 nützt auch eine Zustimmung des Betroffenen nichts ! Letztlich liegt die Entscheidung ob die Zulässigkeit der Ermittlung und Verarbeitung iSd § 7 DSG 2000 gegeben ist, beim ordentlichen Gericht (für den privaten Bereich).

²³⁶ ÖZW, 1979/1, 12ff

6. Die Zulässigkeit der Datenverarbeitung

§ 4 Z 9 DSG 2000 definiert was unter Verarbeiten von Daten zu verstehen ist:

- Ermitteln (= Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden)
- Erfassen
- Speichern
- Aufbewahren
- Ordnen
- Vergleichen
- Verändern
- Verknüpfen
- Vervielfältigen
- Abfragen
- Ausgeben
- Benützen
- Überlassen (= Weitergabe von Daten vom Auftraggeber an einen Dienstleister)
- Sperren
- Löschen
- Vernichten
- oder jede andere Art von Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels von Daten.

6.1. Zweck und Inhalt bestimmt

Allererst müssen gem. § 7 Abs 1 DSG 2000 „Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggeber gedeckt“ sein. Hier wird auf einen Vergleich zu den Tatbestandsvoraussetzungen für die Ermittlung von Daten und deren Verarbeitung abgestellt. Nach der Praxis der DSK musste die Beurteilung des Vorliegens eines berechtigten Zwecks unter Heranziehung der gesamten Rechtsordnung erfolgen.²³⁷ (siehe oben Kapitel 5.2.)

²³⁷ DSK 12.4.1984, ZfVBdat 1986/3/4

6.2. Die schutzwürdigen Geheimhaltungsinteressen

Weiters dürfen die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Das Kriterium der Nichtverletzung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen wird in § 8 DSG 2000 für die nicht-sensiblen Daten präzisiert:

Diese wiederum werden im Sinne des § 8 Abs 1 DSG 2000 dann nicht verletzt wenn

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder (Z 1)
- der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder (Z 2)
- lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder (Z 3)
- überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. (Z 4)

Abs 2 enthält sodann zwei Fälle, in denen schutzwürdige Geheimhaltungsinteressen keinesfalls verletzt sind, nämlich die Verwendung zulässigerweise veröffentlichter Daten und die Verwendung von nur indirekt personenbezogenen Daten.

Abs 3 enthält wiederum eine Präzisierung des vierten Tatbestandes des Abs 1, und zwar in Form einer demonstrativen Aufzählung von sieben Fällen, in denen schutzwürdige Geheimhaltungsinteressen nicht verletzt sind.²³⁸ Die aufgezählten Fälle haben hier weniger die Bedeutung einer konkreten Zulassungsvoraussetzung sondern sollen als „Leitschnur“ bei der Interessensabwägung dienen. In diesen Fällen gibt es keine überwiegenden Rechte des

²³⁸ § 8 Abs 3 DSG 2000 lautet:

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder
5. zur Geltendmachung, Ausübung Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
7. 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 ist; im letztgenannten Fall gilt § 48a Abs 3.

Auftraggebers oder eines Dritten, sondern ist die Verletzung von schutzwürdigen Geheimhaltungsinteressen generell im vorn hinein ausgeschlossen.

Eine andere Meinung hiezu meint jedoch, da § 8 Abs 3 dem § 8 Abs 1 Z 4 DSG 2000 ungeordnet ist auch hier eine Interessensabwägung als notwendig erscheint obwohl dies von der Datenschutz RL nicht verlangt wird und vom Gesetzgeber die Umsetzung (offensichtlich) nicht richtig erfolgt ist.²³⁹

Wirtschaftliche Interessen kommen nur in Frage, wenn sie von der Rechtsordnung auch zu berechtigten Interessen erhoben wurden. Dabei ist eine verfassungsrechtliche Verankerung von Interessen als Indiz für das Überwiegen von Interessen anzusehen: So kann zB das Grundrecht auf Informationsfreiheit (Art 10 EMRK)²⁴⁰ bei der Interessensabwägung bezüglich Personen des öffentlichen Lebens zu einem Überwiegen und damit zu einer Durchbrechung des Geheimhaltungsanspruchs führen.

Die Datenschutz RL nennt in Art 7 lit b ausdrücklich auch die Zulässigkeit der Datenverarbeitung zu vorvertraglichen Maßnahmen, die auf Antrag der betroffenen Person erfolgen. Diese Regelung wurde jedoch nicht in die Aufzählung des § 8 Abs 3 DSG 2000 übernommen. Da die darin gemachten Aufzählungen nur demonstrativen Charakter haben, wird dadurch eine Datenverarbeitung zu vorvertraglichen Maßnahmen ebenfalls ein tauglicher Rechtfertigungsgrund sein. (mit oder ohne Interessensabwägung iSd § 8 Abs 1 Z 4 DSG 2000)

Für das Erfordernis einer Bonitätsprüfung kommt daher nur Z 4 in Betracht, die die Verletzung bei der Erfüllung einer vertraglichen Verpflichtung ausschließt.

Abs 4 bildet eine Sondervorschrift für Daten über gerichtliche oder verwaltungsbehördliche strafbare Handlungen und Unterlassungen.²⁴¹

²³⁹ Dammann/Simitis, EG DS-RL, 148; Duschaneck/Rosenmayr-Klemenz, DSG 2000, 47

²⁴⁰ Artikel 10 - Freiheit der Meinungsäußerung

(1) Jedermann hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Dieser Artikel schließt nicht aus, dass die Staaten Rundfunk-, Lichtspiel- oder Fernsehunternehmen einem Genehmigungsverfahren unterwerfen.

(2) Da die Ausübung dieser Freiheiten Pflichten und Verantwortung mit sich bringt, kann sie bestimmten, vom Gesetz vorgesehenen Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, wie sie in einer demokratischen Gesellschaft im Interesse der nationalen Sicherheit, der territorialen Unversehrtheit oder der öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung und der Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufes oder der Rechte anderer unentbehrlich sind, um die Verbreitung von vertraulichen Nachrichten zu verhindern oder das Ansehen und die Unparteilichkeit der Rechtsprechung zu gewährleisten.

²⁴¹ Grabenwarter, ÖJZ 2000, 866

6.2.1. Die gesetzliche Ermächtigung oder Verpflichtung

An gesetzlichen Ermächtigungen oder Verpflichtungen iSd § 8 Abs 1 Z 1 2000 (überwiegend in Stellen des öffentlichen Bereiches) sind zB anzuführen, Meldepflichten von Beschäftigten an die gesetzlichen Sozialversicherungsträger iSd der §§ 33 bis 43 ASVG, § 26 AuslBG betreffend Auskünfte aus den Unterlagen über ausländische Beschäftigte, etc.

Andererseits gibt es auch gesetzliche Bestimmungen die relativ vage Pflichten von Unternehmen enthalten, bei denen unklar ist welche Daten dafür konkret verarbeitet werden dürfen bzw. müssen. Ein Beispiel ist § 39 BWG Abs 2 und 2a²⁴² der den Banken Sorgfaltspflichten auferlegt und sogar ausdrücklich die Einrichtung von entsprechenden Verwaltungs-, Rechnungs- und Kontrollverfahren verlangt, um das Risiko der Bank beurteilen zu können. Offensichtlich ist dadurch eine Art Bonitätsbeurteilung von Bankkunden in einem gewissen Rahmen gemeint. Welche und wie Daten daher konkret verarbeitet werden dürfen, ist aus dieser Bestimmung nicht ersichtlich. Bis dato ist es unklar, in welchem Umfang die Bonitätsbeurteilung von Bankkunden eine gesetzliche Pflicht, oder im überwiegenden berechtigten Interesse der Bank liegt oder wenn keines von beiden vorliegt, nur nach (widerruflicher) Zustimmung erfolgen kann.²⁴³

²⁴² § 39 Abs 2 BWG lautet: *Die Kreditinstitute haben für die Erfassung, Beurteilung, Steuerung und Überwachung der bankgeschäftlichen und bankbetrieblichen Risiken über Verwaltungs-, Rechnungs- und Kontrollverfahren zu verfügen, die der Art, dem Umfang und der Komplexität der betriebenen Bankgeschäfte angemessen sind. Die Verwaltungs-, Rechnungs- und Kontrollverfahren haben weitest gehend auch bankgeschäftliche und bankbetriebliche Risiken zu erfassen, die sich möglicherweise ergeben können. Die Organisationsstruktur hat durch den Geschäftsbetrieb angemessene aufbau- und ablauforganisatorische Abgrenzungen Interessens- und Kompetenzkonflikte zu vermeiden. Die Zweckmäßigkeit dieser Verfahren und deren Anwendung ist von der internen Revision mindestens einmal jährlich zu prüfen.*

(2a) Kreditinstitute können sich für die Entwicklung und laufende Wartung von Rating-Verfahren gemeinsamer Risikoklassifizierungseinrichtungen als Dienstleister bedienen, wenn sie dies der FMA zuvor angezeigt haben. Die Überlassung aller für die Erfassung und Beurteilung von Risiken erforderlichen Informationen durch die teilnehmenden Kreditinstitute an die gemeinsame Risikoklassifizierungseinrichtung ist zu dem ausschließlichen Zweck zulässig, durch Verarbeitung dieser Daten Verfahren zur Risikobeurteilung und Risikobegrenzung zu entwickeln und laufend zu warten und diese Verfahren den teilnehmenden Kreditinstituten zur Verfügung zu stellen; die Übermittlung von personenbezogenen Daten durch die Risikoklassifizierungseinrichtung ist nur an das Kreditinstitut zulässig, das die zu Grunde liegenden Schuldnerdaten eingemeldet hat. Die gemeinsame Risikoklassifizierungseinrichtung, ihre Organe, Bediensteten und sonst für sie tätigen Personen unterliegen dem Bankgeheimnis gemäß § 38. Die FMA hat in Bezug auf die gemeinsame Risikoklassifizierungseinrichtung alle in § 70 Abs. 1 genannten Auskunfts-, Vorlage- und Prüfungsbefugnisse; § 71 ist anzuwenden.

²⁴³ Knyrim, Datenschutzrecht, 162 (FN 374 f)

6.2.2. Die Zustimmung

Im Falle der Zustimmung zur Übermittlung (§ 8 Abs 1 Z 2 DSG 2000) hat sie durch den Betroffenen im Sinne des § 4 Z 14 DSG 2000 ohne Zwang und in Kenntnis der Sachlage im konkreten Fall zu erfolgen. Da im DSG 2000 keine Unterscheidung mehr zwischen öffentlichen und privatem Bereich gegeben ist und es dadurch nur noch eine datenschutzrechtliche Zustimmung gibt und nicht wie im „alten DSG 1978“ noch zwischen einer öffentlich-rechtlichen²⁴⁴ und einer zivilrechtlichen Zustimmung unterschieden wurde, wird diese jetzt nur noch im Sinne des bürgerlichen Rechts verstanden.²⁴⁵

Das bedeutet, dass ein bloßes Fehlen von Zwang oder Drohung nicht ausreicht, was die in anderen fremdsprachlichen Fassungen der Richtlinie gewählte Formulierung – zB im Englischen: „*freely given indication*“ – besser und deutlicher zum Ausdruck bringt. Eine Zustimmung kann daher insbesondere auch dadurch unwirksam werden, wenn der Betroffene durch ein (wirtschaftliches) Abhängigkeitsverhältnis in seiner freien Disposition beeinflusst wird.²⁴⁶ Zu einer „*Verdünnung der Willensfreiheit*“ wird es regelmäßig dann kommen, wenn zwischen den beteiligten Verhandlungspartnern ein erhebliches wirtschaftliches Ungleichgewicht besteht. Hat nun einer der Partner ein derartiges Gewicht, sodass er den Vertragsinhalt de facto einseitig bestimmen, verkehrt sich die Selbstbestimmung in eine Fremdbestimmung.²⁴⁷ Das deutsche BVerfG²⁴⁸ führt dazu in einer Entscheidung aus, „*dass eine solche Bestimmungsmacht gerade dann vorliegt, wenn die vom überlegenen Vertragspartner angebotene Leistung für den anderen Partner zur Sicherung seiner wirtschaftlichen Existenz von erheblicher Bedeutung ist.*“

Diese Definition ergibt sich aus Art 7 lit a der Datenschutz RL in dem es heißt, dass „die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn (...): a) Die betroffene Person (...) ohne jeden Zweifel ihre Einwilligung gegeben (hat)“, zum anderen wird im Zusammenhang mit der „*Einwilligung*“ auch auf Art 2 lit h verwiesen, demzufolge der Begriff der „*Einwilligung*“ definiert wird als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.“

²⁴⁴ Zum Begriff der öffentlich-rechtlichen Willenserklärung siehe *Raschauer*, Verwaltungsrecht, Rz 1266f

²⁴⁵ GZ K211.634/0004-DSK/2006 vom 14. Februar 2006

²⁴⁶ *Appl*, Der Gläserne Schuldner, Mobiliarpfandregister und Datenschutz, NZ 2007/44

²⁴⁷ zB Zustimmung zur Datenverwendung in Bank AGB: OGH 22.3.2001 4 Ob 28/01y

²⁴⁸ BVerfG 23.10.2006, 1 BvR 2027/02, Rz 35ff

Vom DSG her ist somit eine Willensbekundung möglich, die mangels des Erfordernisses der Ausdrücklichkeit auch konkludent erfolgen kann.²⁴⁹ Von einer stillschweigenden, konkludenten oder schlüssigen Willenserklärung wird dann gesprochen, „wenn der Erklärungswert weniger aus bestimmten Worten oder aus einem bestimmten Verhalten, sondern mehr aus den Begleitumständen erschlossen wird.“²⁵⁰ Schweigen des Betroffenen kann allerdings in eng begrenzten Ausnahmefällen als „Zustimmung“ angesehen werden.²⁵¹ Klar ist jedoch, dass Unterlassungen wie das Schweigen, nicht als ausreichend angesehen werden, wo eine ausdrückliche Zustimmung erforderlich ist.²⁵²

Bei einer Zustimmungserklärung zur Übermittlung der Daten, müssen nach einer Entscheidung des OGH²⁵³ die zu übermittelnde Datenart, der Empfänger und der Übermittlungszweck beinhaltet sein. Auf elektronischem Wege ist nach herrschender Auffassung das dementsprechende „klicken“ auf Antwortfelder bei interaktiven Diensten grundsätzlich für eine gültige Zustimmung ausreichend wenn vorher ausreichende Informationen diesbezüglich gegeben wurden.²⁵⁴ Die Zustimmungserklärung muss auch grafisch besonders hervorgehoben werden. Auf die Möglichkeit der Untersagung ist ausdrücklich und schriftlich hinzuweisen wenn die Daten vom Betroffenen ermittelt werden.²⁵⁵

Der Auftraggeber bzw. Verantwortliche der Verarbeitung hat dem Betroffenen die benötigten Informationen wie Name und Anschrift des Verantwortlichen, Zweck der Verarbeitung, gespeicherte Daten usw. über die beabsichtigte Datenverwendung mitzuteilen. Die Einwilligung hat zwar Fall bezogen zu erfolgen doch ist sie primär als „zweckbezogen“ anzusehen. Damit soll erreicht werden, dass nicht bei mehreren Datenverwendungen stets eine neue Zustimmung eingeholt werden muss, sondern der Zweck der Verwendung und die Person des Verantwortlichen in der Zustimmung ausreichend bestimmt ist und danach nicht gewechselt werden darf.

²⁴⁹ Grabenwarter, ÖJZ 2000, 867; dazu auch Dammann/Simitis, EG DS-RL, 148; Schleutermann, Datenverarbeitung im Konzern, CR 1995, 555 [579]

²⁵⁰ Koziol-Welser, Grundriss, 13. Aufl, 101ff; zu beachten ist jedoch die Zweifelsregel in § 863 Abs 1 2. Halbsatz ABGB wonach der Erklärungswert zweifelsfrei feststehen muss

²⁵¹ So Dammann/Simitis, EG DS-RL, 115; aA Brühmann, DuD 1996, 66 u. 69 welcher jedoch die Möglichkeit einer konkludenten Zustimmung ausschließt

²⁵² Reimer, in Jahnel/Sieglwart/Fercher, Aktuelle Fragen des Datenschutzrechts, 205ff der Schweigen grundsätzlich als Zustimmung im DSG ausschließt da im Zivilrecht eine Widerspruchspflicht Voraussetzung für die Zulässigkeit einer konkludenten Willenserklärung durch Schweigen ist; dazu wiederum Koziol/Welser, Grundriss 13. Aufl., 103

²⁵³ OGH 22.3.2001 4 Ob 28/01y = SZ 74/52

²⁵⁴ aA wiederum Brühmann (FN 251)

²⁵⁵ OGH 27.1.1999 7 Ob 326/98m; Feuchtinger, Erleichterungen bei den Meldepflichten nach dem DSG, SWK 2000, W 109; eine vollständige Darstellung der Judikatur siehe bei Knyrim, Datenschutzrecht (2003), 178

Die Wirksamkeit der Zustimmung hängt demgemäß maßgeblich davon ab, ob der Auftraggeber seinen Informationspflichten insbesondere nach den §§ 24 und 26 DSG 2000 bzw. den Art 10 Datenschutz RL in gesetzkonformer Weise nachkommt.

Dammann/Simitis gehen in ihren Ausführungen von einem „*beweglichen System*“ aus. Dies bedeutet, dass je größer die Tragweite der Erklärung für die Rechte und Freiheiten der betroffenen Person ist, umso höher sind die Anforderungen an ihre Bestimmtheit. Diesen Ausführungen ist in meinen Augen zuzustimmen, weil davon ausgegangen werden kann, dass die betroffenen Personen die Einsicht und das Wissen haben, bei gravierenden Erklärungen größere Sorgfalt walten zu lassen als in Bagatellangelegenheiten.²⁵⁶

Gleichzeitig muss jedoch auch festgehalten werden, dass oft Zustimmungen verlangt werden, die eigentlich gar keine Zustimmungen iSd § 1 Abs 2 DSG 2000 sind, weil der Eingriff bereits auf Grund überwiegender berechtigter Interessen eines anderen legitimiert ist. Die zustimmungsgebundenen Schutzbestimmungen wie zB die jederzeitige Widerrufbarkeit oder die Zwangsfreiheit, sind in diesen Fällen nicht anwendbar.²⁵⁷

Sie darf sich nicht aus Allgemeinen Geschäftsbedingungen (AGB's) ergeben sondern muss dem Betroffenen bewusst werden (zB in Form einer gesonderten Zustimmungserklärung, auf einem Antrag oder unmittelbar vor der Unterschrift des Betroffenen unter einem Vertrag). Sie ist jederzeit widerrufbar (in Analogie zu § 860a ABGB) und bewirkt die Unzulässigkeit der Verwendung der Daten (§ 8 Abs 1 Z 2 DSG 2000). Ab dem Widerruf dürfen keine weiteren Übermittlungen mehr erfolgen, außer es ist ein anderer Übermittlungsgrund angegeben. Sowohl die Zustimmungserklärung als auch der Widerruf können bedingt, eingeschränkt (zB an genaue Empfänger, Datenarten, etc.) oder befristet erfolgen. Weiters ist zu beachten, dass die „interne“ Weitergabe von Daten eines Unternehmens an zB ein Tochterunternehmen eine Übermittlung iSd § 7 Abs 2 DSG 2000 darstellt.

Prinzipiell ist bei Zustimmungserklärungen folgendes zu beachten:

- Zustimmungserklärungen dürfen NICHT in AGB „versteckt“ werden, sondern müssen von diesen deutlich getrennt werden

²⁵⁶ Grabenwarter, ÖJZ 2000, 868

²⁵⁷ Reimer in Jähnel/Siegrwart/Fercher, Aktuelle Fragen des Datenschutzrechts, 210

- Zustimmungserklärungen dürfen nicht pauschal auf AGB verweisen
- Zustimmungserklärungen müssen deutlich lesbar sein zB in Form einer Hervorhebung
- Zustimmungserklärungen müssen gesondert unterschrieben werden

Zum Inhalt einer ausdrücklichen Zustimmungserklärung hat der Verfassungsdienst²⁵⁸ festgehalten, dass eine Zustimmungserklärung folgende Angaben enthalten muss:

- Die genaue Bezeichnung der Datenarten (zB Name, Geburtsdatum, Adresse,..) nicht nur „persönliche Daten“
- Die Benennung der Übermittlungsempfänger (Name, Adresse, Behördenbezeichnung,...)²⁵⁹
- Eine ausreichende Information über den Übermittlungszweck
- Einen ausdrücklichen Hinweis²⁶⁰ auf den jederzeit möglichen schriftlichen Widerruf

²⁵⁸ Rundschreiben des BKA-VD, 810.008/1-V/11a/85 vom 10.8.1985, abgedruckt bei *Dohr/Pollirer/Weihs*, DSG, Anh IV/2 2

²⁵⁹ OGH 22.3.2001 4 Ob 28/01 y = ecolex 2001/147 = ÖBA 2001/977 = RdW 2001/557

²⁶⁰ OGH 19.11.2002 5 Ob 179/02 f = SZ 2002/153

Die DS-RL unterscheidet zwischen Verarbeitungen auf Grund einer Einwilligung und zur Erfüllung eines Vertrages. Dies ist insoweit interessant, als die im Rahmen von Verträgen abgegebenen Zustimmungserklärungen besondere Rechtsprobleme in Bezug auf jederzeitige Widerrufbarkeit und ihre Folgen aufwerfen (können):

Art 7		Art 8	
lit a	Zustimmung des Betroffenen	Abs 2 lit a	Zustimmung des Betroffenen
lit b	überwiegende berechtigte Interessen anderer	Abs 2 lit b	überwiegende berechtigte Interessen anderer
lit c	Überwiegende berechtigte Interessen anderer	Abs 2 lit c	Lebenswichtige Interessen des Betroffenen bzw. überwiegende berechtigte Interessen anderer
lit d	Lebenswichtige Interessen des Betroffenen	Abs 2 lit d	überwiegende berechtigte Interessen anderer
lit e	überwiegende berechtigte Interessen anderer	Abs 2 lit e	Zustimmung des Betroffenen bzw. überwiegende Interessen anderer
lit f	überwiegende berechtigte Interessen anderer	Abs 3	überwiegende berechtigte Interessen anderer

Daraus ist ersichtlich, dass die innerstaatliche Unterscheidung zwischen einem Vertrag und einer Zustimmung als Rechtsgrundlage für eine Datenverwendung nur für sensible Date in § 9 DSG 2000 explizit beibehalten wurde. Dennoch ist eine richtlinienkonforme Interpretation möglich, da § 8 Abs 3 DSG 2000 ausdrücklich eine demonstrative Aufzählung enthält (arg: „insbesondere“). Somit kann aus dem fehlenden Verweis auf vertragliche Bestimmungen im Katalog des § 8 DSG 2000 nicht geschlossen werden, dass Verträge als Zustimmung gemäß § 8 Abs 1 Z 2 DSG 2000 anzusehen sind.

Reimer²⁶¹ unterscheidet in weiterer Folge zwischen Fällen „echter Zustimmung“ und Fällen „unechter Zustimmung“. Die Unterscheidung lässt sich leicht anhand der Erforderlichkeit bemessen: Ist die Verwendung der Daten zur Erfüllung vertraglicher Pflichten notwendig, handelt es sich um einen Fall der „unechten Zustimmung“, da der Eingriff bereits aufgrund „überwiegender berechtigter Interessen eines anderen“ zulässig ist. Ist die Verwendung der Daten nicht zur Erfüllung vertraglicher Pflichten notwendig, etwa weil die einzige Pflicht in

²⁶¹ Reimer in Jähnel/Sieghart/Fercher, Aktuelle Fragen des Datenschutzrechts, 196ff

der Duldung des Eingriffs besteht oder der Eingriff über das zur Erfüllung der anderen vertraglichen Verpflichtung erforderliche Maß hinausgeht, dann ist eine „*echte Zustimmung*“ erforderlich.

Die Beurteilung der Zulässigkeit der Datenverarbeitung unter den Bedingungen des § 8 Abs 1 Z 4 DSG 2000 hat im Rahmen des § 7 DSG 2000 so statt zu finden, dass „Zweck und Inhalt der Datenanwendung“ die schutzwürdigen Geheimhaltungsinteressen nicht verletzen. Dies bedeutet aber auch in weiterer Folge, dass nicht bloß Zweck und Inhalt der Verarbeitung, sondern auch jener einer späteren Übermittlung zu beachten ist und ggf. iSd des § 8 Abs 1 Z 4 DSG 2000 einzustellen ist. Die Abwägung der Interessen des Auftraggebers bzw. des Dritten und des Betroffenen erfordert eine Bewertung der konkret involvierten Interessen. Diese Bewertung darf nur anhand der Wertentscheidungen der Rechtsordnung vorgenommen werden.

Auf der Seite des Betroffenen ist das Interesse an der Geheimhaltung seiner Daten zu veranschlagen. Dieses wird mit dem Inhalt und der Eingriffstiefe höher werden. So werden bei allgemein zugänglichen/öffentlichen Daten wie zB Name, Adresse, Telefonnummer die Geheimhaltungsinteressen geringer sein als bei Daten über Einkommen, finanzielle Situation oder ähnliches.

Aber Abs 3 Z 4 umschließt in der Erforderlichkeit nicht nur die vertraglichen Hauptpflichten sondern auch Nebenpflichten welche auch daher selbständig Grundlage für eine Datenverarbeitung sein können. Diese Nebenpflichten umfassen auch eine Rücksichtnahme auf die Interessen und Usancen des Vertragspartners, sodass eine Datenverarbeitung welche die Rechte und Freiheiten der betroffenen Person nicht tangiert, im weiteren Sinn erforderlich und daher als zulässig angesehen werden kann. Als Richtschnur kann auch § 28 Abs 1 Nr 1 des deutschen BDSG 2003 dienen welches von „*der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient*“, spricht.²⁶²

Eine Zustimmung für die Zukunft ist auch möglich wenn die Zustimmungserklärung nach betroffenen Daten und Aktivitäten näher umschriebenen Inhalt und Umfang hat. Daher kann innerhalb eines bestimmten Rahmens – nämlich der von Datenarten und Verarbeitungszweck – die Zustimmung für die Zukunft erteilt werden.²⁶³

²⁶² Grabenwarter, ÖJZ 2000, 869 sowie Dammann/Simitis, EG DS-RL, 149

²⁶³ Dammann/Simitis, EG DS-RL, 115; Knyrim, Datenschutzrecht, 185

Weiters besteht ein datenschutzrechtliches „*Koppelungsverbot*“. Darunter versteht man das Verbot, die Erbringung von Leistungen von der Zustimmung in die Verwendung der Daten abhängig zu machen obwohl dieses in Österreich nicht ausdrücklich gesetzlich normiert ist. Dennoch gibt es einige einfachgesetzliche Bedingungen, die Koppelungen ausdrücklich verbieten, ohne dies „*Koppelungsverbot*“ zu nennen.²⁶⁴

- nach § 31a Abs 4a 2. Satz ASVG *“einen Anspruch des Karteninhabers [...] von der Verwendung von Bestandteilen des ELSY [...] abhängig zu machen oder inhaltlich zu beeinflussen*²⁶⁵
- § 96 Abs 2 letzter Satz TKG 2003 *„die Anbieter [...] die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen [dürfen]*
- § 30 Abs 3 letzter Satz ZustG *„der Abschluss eines Vertrages über die Zustellung [...] nicht von der Zustimmung zur Weitergabe von Daten an Dritte abhängig gemacht oder inhaltlich beeinflusst werden [darf].*

Damit betont der einfache Gesetzgeber, dass es keine „überwiegende berechtigte Interessen eines anderen“ gibt, da hiemit die Entscheidungsfreiheit des Betroffenen besonders abgesichert wird. Wo jedoch „überwiegend berechtigte Interessen eines anderen“ vorliegen, dürfen Zustimmungen auch verlangt werden.²⁶⁶

So ergibt sich aus dem im § 6 Abs 1 Z 1 DSG 2000 festgelegten Grundsatz, wonach Daten *„nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden dürfen“*. Dieser Grundsatz fordert eine möglichst umfassende Information, um es dem Betroffenen zu erleichtern, seine Rechte zu wahren. Dazu gehört auch die Information über die durch § 8 Abs 1 Z 4 DSG 2000 eingeräumte Möglichkeit, eine bereits erteilte Zustimmung zur Datenweitergabe zu widerrufen. Diese gegenüber anderen Rechtsbereichen *„erweiterte“* Informationspflicht ist auch aus § 24 DSG 2000 abzuleiten, einer Bestimmung, die nach den Materialien²⁶⁷ den Betroffenen in die Lage versetzen soll, das Vorhandensein einer Verarbeitung zu erfahren und umfassend über die Bedingungen der Erhebung informiert zu sein. Das auf *Koziol*²⁶⁸ gestützte Argument, ein Hinweis auf den Widerruf sei schon deshalb nicht erforderlich, weil § 24 DSG 2000 im Gegensatz zu § 268 Abs 6 GewO einen Hinweis

²⁶⁴ Dazu ausführlich *Reimer in Jahn/Siegrwart/Fercher*, Aktuelle Fragen des Datenschutzrechts, 202ff

²⁶⁵ SRÄG 2006, BGBl Nr 131/2006

²⁶⁶ DSK vom 15.12.2000, 120.715/4-DSK/00 zur rechtmäßigen Übermittlung von Gesundheitsdaten an die Koppelung der Auszahlung von Sozialleistungen

²⁶⁷ Erl RV 1613 BlgNR XX. GP

²⁶⁸ *Koziol*, Haftpflichtrecht I³, Rz 10

auf das Untersagungsrecht des Kunden nicht vorsehe, ist mangels Vergleichbarkeit der Regelungen nicht tragfähig. Vom Recht des Kunden, eine bereits erteilte Zustimmung zur Datenverwendung zu widerrufen, ist das in § 28 DSG 2000 geregelte Widerspruchsrecht zu unterscheiden.²⁶⁹

6.3. Die Zulässigkeit der Datenübermittlung

Nach Art 7 lit f der Datenschutz RL ist die Weitergabe von Daten erlaubt, wenn sie erforderlich ist zur Verwirklichung des berechtigten Interesses, das von dem Dritten wahrgenommen wird, dem die personenbezogenen Daten übermittelt werden, sofern nicht das Interesse oder die geschützten Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Durch die Weitergabe gerät der datenschutzrechtliche Geheimhaltungsanspruch in ein Spannungsverhältnis zur grundrechtlichen Gewährleistung des freien Austausches von Informationen durch die Meinungs- bzw. Kommunikationsfreiheit (Art 13 StGG und Art 10 EMRK). *Berka*²⁷⁰ meint, dass die legitimen öffentlichen Informationsinteressen nicht unverhältnismäßig verkürzt werden dürfen, wenn es sich um einen Sachverhalt von „öffentlichen Belang“ handelt. *Laurer*²⁷¹ wiederum hat aufgrund der Drittwirkung des Grundrechts auf Datenschutz auf dessen Überhang geschlossen obwohl § 48 Abs 2 DSG 2000 die Verwendung von Daten zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechts auf freie Meinungsäußerung gem Art 10 Abs 1 EMRK zulässt, ohne sie den Beschränkungen des Datenschutzrechts zu unterwerfen. Offensichtlich wird hier vom Vorliegen überwiegend berechtigter (Informations-) Interessen anderer iSd § 1 Abs 2 1. Satz DSG 2000 ausgegangen (sog. „Medienprivileg“)²⁷².

Der eigentliche harte Kern auch des neuen Datenschutzgesetzes ist die grundsätzliche Unzulässigkeit der Übermittlung (siehe hiezu § 4 Z 12 DSG 2000) von Daten bzw. deren eingeschränkte Erlaubnis normiert im 2. Abschnitt in den §§ 6 bis 9 DSG 2000.

Bei der Übermittlung, das ist die Weitergabe von Daten an andere Empfänger als den Betroffenen selbst oder den Auftraggeber bzw. Dienstleister (siehe hiezu § 4 Z. 5 DSG 2000)

²⁶⁹ In diesem Sinne OGH 19.11.2002 4 Ob 179/02f = SZ 2002/153 der festhält, dass „die dem Betroffenen eröffnete Widerrufsmöglichkeit [...] zentraler Bestandteil des aus seiner Zustimmung folgenden Schutzes [sei]. Seine Nichterwähnung vermittele dem Verbraucher ein unklares Bild seiner vertraglichen Position und könne dazu führen, dass er in Unkenntnis seiner Rechte an ihrer Ausübung gehindert werde, zumal die Kenntnis der Widerrufsmöglichkeit nicht vorausgesetzt werden könne“

²⁷⁰ *Berka* in *Korinek/Holoubek* (Hrsg), Österr BfVR, 452

²⁷¹ *Laurer*, Der Geheimnisschutz im österreichischen Grundrechtssystem, EuGRZ 1983, 37

²⁷² *Dohr/Pollirer/Weiss*, § 48 Anm 5; *Duschanek/Rosenmayr-Klemen*, 148ff

ist zwischen der externen und internen Weitergabe zu unterscheiden. Unter „Veröffentlichen“ welche eine Form der Datenübermittlung darstellt, versteht man dagegen die Weitergabe an einen unbestimmten Adressatenkreis oder wie die DSK feststellt, *„Daten welche in der Absicht möglichst breiter Kenntnisnahmen durch unbestimmte Dritte an öffentlich zugänglichen Orten zur Schau gestellt werden“*.²⁷³

Aufgrund einer rechtdogmatischen Analyse des § 7 Abs 2 Z 2 DSG 2000 verhindert dieser eigentlich die Datenveröffentlichung weil auf den Übermittlungsempfänger und seine rechtliche Befugnisse nicht abgestellt werden kann und der Geheimhaltungsanspruch in diesem Falle grundsätzlich entfällt. Da dem Gesetzgeber die Unkenntnis der Veröffentlichung nicht unterstellt werden kann, indem er sie ja in § 4 Z 12 DSG 2000 aufzählt, bleibt aufgrund der sachlich gerechtfertigten unterschiedlichen Behandlung von Weitergabe und Veröffentlichung, nur die Möglichkeit § 7 Abs 2 Z 2 DSG 2000 im Falle der Veröffentlichung, teleologisch zu reduzieren und nicht anzuwenden.²⁷⁴

Keine Beschränkungen legt das DSG 2000 im privaten Bereich auf bei

- a. Weitergabe an Abteilungen oder andere Unternehmensteile wie Filialen etc., sofern es sich um das selbe Aufgabengebiet handelt; andernfalls müssen die Voraussetzungen des § 7ff DSG 2000 gegeben sein (siehe hiezu auch OGH 4 Ob 114/91 vom 25.2.1991). Um jedoch die Zulässigkeit solcher Datenübermittlungen außer Zweifel zu stellen, sollte dies in der Rechtsgrundlage für die jeweils bestehenden Unternehmensverflechtungen ausdrücklich verankert werden. (zB mit Hinweisen auf eine gemeinsame Verkaufs- oder Personalverwaltungsorganisation)
- b. Mitteilung der Daten an den Betroffenen selbst
- c. Weitergabe von eigenen Unternehmensdaten an Dritte (jedoch heikel weil andere Personen nicht mit betroffen sein dürfen)

²⁷³ GZ K121.046/0016-DSK/2005 vom 29. November 2005; GZ K120.867/0001-DSK/2004 vom 27. Februar 2004

²⁷⁴ So auch Siegart in Jahnel (Hrsg), Aktuelle Fragen des Datenschutzrechts, 238ff

- d. Bei Verwendung ausschließlich im privaten oder familiären Bereich wenn sie vom Betroffenen selbst mitgeteilt worden sind oder sonst rechtmäßig im Sinne des § 7 Abs 2 DSG 2000 zugekommen sind Bei Verwendung für andere Zwecke ist wiederum die Zustimmung des Betroffenen einzuholen (§ 45 DSG 2000).

Die Übermittlung (und daher auch die Veröffentlichung) von Daten ist daher nur zulässig wenn

- a) die Daten aus einer zulässigen Datenverarbeitung stammen UND
- b) der Empfänger über eine ausreichende gesetzliche Zuständigkeit bzw. rechtliche Befugnis verfügt UND
- c) durch Zweck und Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen im Sinne der §§ 8 und 9 DSG 2000 nicht verletzt werden.

Das DSG 2000 misst dadurch, dass es in seinem § 18 Abs 2 Z 3 DSG 2000 Datenanwendungen, die die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben, für vorabkontrollpflichtig erklärt, Bonitätsdaten eine besondere Eingriffstiefe in das Recht auf Geheimhaltung (§ 1 Abs 1 DSG 2000) zu. Diese Konstellation erfordert besondere Sorgfalt seitens der Kreditauskunfteien ebenso wie seitens ihrer Datenlieferanten. Daher muss geprüft werden, ob Daten, die auf den ersten Blick bonitätsrelevant scheinen, in Wahrheit keine oder nur sehr beschränkte/unzuverlässige Aussagekraft über die Bonität des Betroffenen zukommt.

Ob solche Umstände vorliegen, muss geprüft werden, bevor Daten von einer Kreditauskunftei verarbeitet oder an eine solche übermittelt werden. In diesem Zusammenhang ist auch der sachlichen Datenrichtigkeit (§ 6 Abs 1 Z 4 DSG 2000) besondere Bedeutung zuzumessen: Diese muss im Hinblick auf den Verwendungszweck einer Bonitätsauskunft gegeben sein. Liegt sie nicht (mehr) vor, ist ein überwiegendes berechtigtes Interesse an der Übermittlung dieser Daten an eine Kreditauskunftei nicht gegeben. Damit der Auftraggeber diesen Obliegenheiten genügen kann, kommt seinen Informationspflichten nach § 24 Abs 2 DSG 2000 besondere Bedeutung zu, insoweit muss er auch selbst aktiv werden.

Der Gesetzgeber hat in § 152 GewO Regeln für Auskunfteien über Kreditverhältnisse aufgestellt. Daraus ist zu schließen, dass der Gesetzgeber von der grundsätzlichen Zulässigkeit dieser gewerblichen Tätigkeit ausgeht, sodass es zur Verarbeitung dieser Daten eine rechtliche Befugnis im Sinne des § 7 Abs 1 DSG 2000 geben kann. Da die Ausübung

dieser gewerblichen Tätigkeit ohne Sammlung, Aufbewahrung und Weitergabe von entsprechenden Daten nicht sinnvoll vorstellbar ist, muss auch angenommen werden, dass der Gesetzgeber in bestimmten Fallkategorien ein die Betroffeneninteressen überwiegendes berechtigtes Interesse dieser Gewerbetreibenden an einer Verwendung von Daten über „Kreditverhältnisse“ im Sinn des § 1 Abs 2 bzw § 8 Abs 1 Z 4 DSG 2000 als gegeben erachtet. Ein derartiges Interesse bzw eine derartige Befugnis muss auch für die Kunden der Auskunftfeien aber auch für die Datenlieferanten bestehen, da ansonsten die Gewerbeausübung unmöglich wäre (vgl auch den 2. Satz des § 1052 ABGB²⁷⁵, der ebenfalls erkennen lässt, dass von einem berechtigten Interesse der Gläubiger an der Verwendung von Bonitätsdaten auszugehen ist).²⁷⁶

§ 4 Z 12 DSG 2000 definiert das Übermitteln von Daten als

Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder den Dienstleister

- insbesondere auch das Veröffentlichen solcher Daten,
- darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

§ 7 Abs 2 DSG 2000 nennt als Vorbedingung für jede Übermittlung, dass die Verarbeitung im Sinne des § 7 Abs 1 DSG 2000 (siehe Kapitel 5.) zulässig sein muss (§ 7 Abs 2 Z 1 DSG 2000) und

a) der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat (§ 7 Abs 2 Z 2 DSG 2000) und

b) durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. (§ 7 Abs 2 Z 3 DSG 2000)

²⁷⁵ § 1052 ABGB lautet: *Wer auf die Übergabe dringen will, muss seine Verbindlichkeit erfüllt haben oder sie zu erfüllen bereit sein. Auch der zur Vorausleistung Verpflichtete kann seine Leistung bis zur Bewirkung oder Sicherstellung der Gegenleistung verweigern, wenn diese durch schlechte Vermögensverhältnisse des anderen Teiles gefährdet ist, die ihm zur Zeit des Vertragsabschlusses nicht bekannt sein mussten.*

²⁷⁶ GZ K211.773/0009-DSK/2007 vom 7. Mai 2007

6.3.1. Die gesetzliche Zuständigkeit oder rechtliche Befugnis

Zweite Voraussetzung ist, dass der Empfänger dem Übermittelnden seine rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft macht. Dieses Erfordernis entfällt, wenn keine Zweifel an der Befugnis bestehen. Damit ist gemeint, dass der Zweck der Übermittlung durch den Auftraggeber im Rahmen der rechtmäßigen Zwecke der Verarbeitung der erhaltenen Daten durch den Empfänger gelegen ist.²⁷⁷

Um hier sicher zu gehen, wird bei Datenbankanfragen betreffend die Kreditwürdigkeit/Bonität oft die (wenn auch rhetorische) Frage gestellt ob man zur Abfrage ein diesbezügliches überwiegendes Interesse oder die Zustimmung des Betroffenen vor-/nachweisen kann. Ein generelles Vorliegen der Voraussetzungen lässt sich vorab nicht für alle Datenübermittlungen bejahen sondern ist im Zuge der Übermittlungen vom Auftraggeber zu beachten weil ihn die Verantwortlichkeit iSd § 7 Abs 2 DSG 2000 trifft.

²⁷⁷ Grabenwarter, ÖJZ 2000, 870

6.3.2. Die schutzwürdigen Geheimhaltungsinteressen

Im dritten und letzten Schritt der Prüfung werden die schutzwürdigen Geheimhaltungsinteressen des Betroffenen abgewogen. Diese Prüfung erfolgt wiederum unter zu Hilfenahme des § 8 Abs 1 DSG 2000. Im Unterschied zu § 7 Abs 1 DSG 2000 sind in dieser Abwägung jedoch nicht Zweck und Inhalt der Datenverwendung insgesamt sondern nur Zweck und Inhalt der Datenübermittlung zu prüfen.

In Betracht kommen hier wiederum die Tatbestände des § 8 Abs 1 Z 2 DSG 2000 („Zustimmung“) bzw Z 4 („überwiegend berechtigte Interessen des Auftraggebers“). Zu Z 2 kann auf die Ausführungen zur Datenermittlung (siehe Kapitel 5.) verwiesen werden. Bei Z 4 ist wiederum eine Interessensabwägung zwischen dem überwiegend berechtigten Interessen des Auftraggebers und den schutzwürdigen Interessen des Betroffenen vorzunehmen.²⁷⁸

Die Technik der Übermittlung ist dabei nicht von Belang. Die Daten werden entweder an Dritte weitergegeben (aktives Verhalten) oder der Dritte nimmt Kenntnis von Daten, die von der verantwortlichen Stelle zur Einsichtnahme oder zum Abruf bereitgehalten werden. (passives Verhalten)

Ein Eingriff in das Recht auf Datenschutz kann nach der gebotenen Interessenabwägung²⁷⁹ gerechtfertigt sein. Bei dieser sind die von der Judikatur zu anderen Interessenkollisionen (zum Beispiel beim Recht auf Meinungsfreiheit nach Art 10 EMRK gegenüber dem Recht auf Ehre nach § 1330 ABGB) entwickelten Grundsätze²⁸⁰ anwendbar. Jeder Weitergabe von Daten (nach § 8 Abs 1 Z 3 DSG 2000) muss eine Interessenabwägung vorangehen zwischen einem schutzwürdigen Interesse des Betroffenen und dem berechtigten Interesse eines Dritten, wobei im Zweifel die Vermutung für die Schutzwürdigkeit spricht. Als berechtigte Interessen Dritter sind dabei ua auch subjektive, auf gesetzlicher oder vertraglich vereinbarter Grundlage beruhende Ansprüche anerkannt.²⁸¹

Der VfGH argumentierte in Bezug auf die Erhebung und Offenlegung von Wirtschaftsdaten,²⁸² an denen die Wirtschaftssubjekte ein schutzwürdiges Interesse haben, dass gemäß § 1 Abs 2 DSG (1978) iVm Art 8 Abs 2 MRK nur zulässig ist, „wenn eine zur

²⁷⁸ Grabenwarter, ÖJZ 2000, 871

²⁷⁹ In den ErläutRV 1613 BlgNR XX. GP wird jedoch ein Vorrang des Grundrechts auf Datenschutz vor anderen Grundrechten ausgeschlossen

²⁸⁰ SZ 64/36

²⁸¹ OGH 6 Ob 148/00h vom 28.6.2000; OGH 2 Ob 244/99t vom 26.8.1999

²⁸² VfSlg 12.228 vom 30.11.1989, G 245-250/89, G 268-275/89; obwohl diese Entscheidung noch zum alten DSG und zur Offenlegung bezüglich des Bezügegesetzes erging, kann daraus eine Zulässigkeit der Erhebung von Wirtschaftsdaten unter bestimmten Voraussetzungen abgelesen werden

Datenerhebung ermächtigende Norm den Informationseingriff gestattet, dieser einem der enumerativ aufgezählten Eingriffsziele dient, auf das Erforderliche beschränkt und einem demokratischen Staat angemessen ist.“

Auch in solchen Fällen muss kraft der ausdrücklichen verfassungsrechtlichen Normierung in § 1 Abs 2 2. Satz DSG (1978) der vertraulichen Behandlung der erhobenen Daten Vorrang gegeben werden, wodurch "der allgemeine Gedanke einer tendenziell geheimnisschutzfreundliche Behandlung" geschützter Daten zum Ausdruck kommt²⁸³ und woraus sich insbesondere auch Beschränkungen der Möglichkeit zur Veröffentlichung von rechtmäßig erhobenen geschützten Daten ergeben.

Statistische Erhebungen von Wirtschaftsdaten sind für die Wirtschaftsforschung und damit für eine heutigen Anforderungen entsprechende Wirtschaftspolitik erforderlich. Die Erhebung von Wirtschaftsdaten ist an sich als iSd § 1 Abs 2 DSG (1978) iVm Art 8 Abs 2 MRK für das wirtschaftliche Wohl eines Landes notwendig und daher verfassungsrechtlich zulässig.

§ 1 Abs 2 DSG (1978) verlangt jedoch, dass Datenerhebungen jedenfalls in zweifacher Hinsicht verhältnismäßig sein müssen:

1. Einerseits darf die Datenerhebung nur in jenem Ausmaß zulässig sein, das im Interesse des wirtschaftlichen Wohles des Landes erforderlich ist; die Tatsache, dass die statistische Erhebung von Wirtschaftsdaten der Wirtschaftsforschung und Wirtschaftspolitik dient und diese im Interesse des wirtschaftlichen Wohles des Landes liegt, bewirkt nicht, dass statistische Erhebungen von Wirtschaftsdaten jedweder Art verfassungsrechtlich zulässig sind.
2. Andererseits muss auch dann, wenn Datenerhebungen zulässig sind, Vorsorge für eine möglichst vertrauliche Behandlung dieser Daten getroffen werden.

Bei überwiegendem berechtigtem Interesse des Auftraggebers oder eines Dritten wird auf die Notwendigkeit der Interessenabwägung zwischen dem Betroffenen und dem Auftraggeber bzw. eines Dritten abgestellt. Die Interessen des Auftraggebers oder eines Dritten müssen berechtigt sein, dh von der Rechtsordnung anerkannt sein und gegenüber dem Betroffenen überwiegen. Damit ist wiederum die Verbindung zum zentralen Begriff des „Unternehmenszweck“ gegeben, der bereits bei der Ermittlung und Verarbeitung

²⁸³ vgl. Rill, Das Grundrecht auf Datenschutz, in: Duschaneck (Hrsg), Datenschutz in der Wirtschaft (1981), 35

ausschlaggebend war.²⁸⁴ Wird daher der Erhalt der Daten für die Erfüllung der Geschäftszwecke notwendig sein, so wird eine Weitergabe zulässig sein. Im Zweifelsfall wird jedoch die Entscheidung zugunsten der Interessen des Betroffenen ausfallen – dies ergibt sich aus der Einordnung in der oben angeführten Skala und der Eingriffsmöglichkeit in gelindesten Form in § 1 Abs 2 letzter Satz DSG 2000. Eine trotz einschlägiger Gewerbeberechtigung getätigte Verarbeitung ist demnach unzulässig wenn sie gegen die schutzwürdigen Interessen des Betroffenen verstößt.

Andererseits sind durch den Auftraggeber zulässig erfasste und gespeicherte Daten nicht automatisch dazu durch diesen berechtigt an einen Dritten übermittelt zu werden. Die Zulässigkeit der Verarbeitung ist bloß eine der Voraussetzungen für die Zulässigkeit der Übermittlung iSd § 7 Abs 2 DSG 2000.

An sich schließt die Verweigerung einer Zustimmung zu einer Übermittlung noch nicht die Möglichkeit einer Übermittlung aufgrund der überwiegend berechtigten Interessen des Auftraggebers oder eines Dritten aus. Da auf die Zulässigkeit der Übermittlung für einen Empfänger abgestellt wird (§ 7 Abs 1 Z 2 DSG 2000) stellt sich jedoch die Frage ob diese Bestimmung, generelle Übermittlungen an eine Evidenzstelle (zB Kreditevidenz, Kfz Haftpflichtversicherung im Rahmen des Bonus-Malus-System), zulässig ist. Da hier noch kein konkretes Interesse eines Dritten feststellbar ist, sondern dieses erst eintreten könnte (Zahlungsausfall, Unfallverursacher) stellt die hL auch auf das überwiegende Interesse einer vom Empfänger verschiedenen Person als Grundlage ab.²⁸⁵

Eine zulässige Übermittlung ist auch gegeben wenn zulässigerweise veröffentlichte Daten oder nur indirekt personenbezogene Daten übermittelt werden (§ 8 Abs 2 DSG 2000). Schon aus der Definition im § 4 Z 1 2. Satz geht hervor, dass diese Daten für den Auftraggeber, Dienstleister oder Empfänger nicht mehr mit rechtlich zulässigen Mitteln bestimmbar sind. Dies bedeutet in weiterer Folge, dass die Übermittlung anonymisiert = ohne individuelle Merkmale, erfolgen muss.

²⁸⁴ aA *Stadler*, Wirtschaftsinformationen, 12ff, versucht zur Beurteilung der Zulässigkeit der Ermittlung und Verarbeitung von Daten diese nach ihrem Naheverhältnis zum Privat- und Familienleben des Betroffenen zu reihen und daraus eine Vermutung der Zulässigkeit abzuleiten; eine klare Antwort auf die verschiedenen Zulässigkeitsfragen kann daraus aber nicht entnommen werden, um so mehr das DSG keine Anhaltspunkte dafür bietet (so auch *Duschanek*, Datenschutzgesetz, 308)

²⁸⁵ ÖZW 1979/1,16

Keine Übermittlung liegt jedoch vor bei ²⁸⁶

- Überlassung von Daten an Dienstleister
- Mitteilung von Daten an den Betroffenen, wobei die Identität des Auftraggebers mitzuteilen ist
- Weitergabe von Daten an Abteilungen oder Zweigstellen innerhalb desselben Unternehmens innerhalb desselben Aufgabenbereiches
- Weitergabe der eigenen Unternehmensdaten an Dritte, sofern dabei nicht fremde Daten (zB Mitarbeiterdaten, Kundendaten) mitgeteilt werden

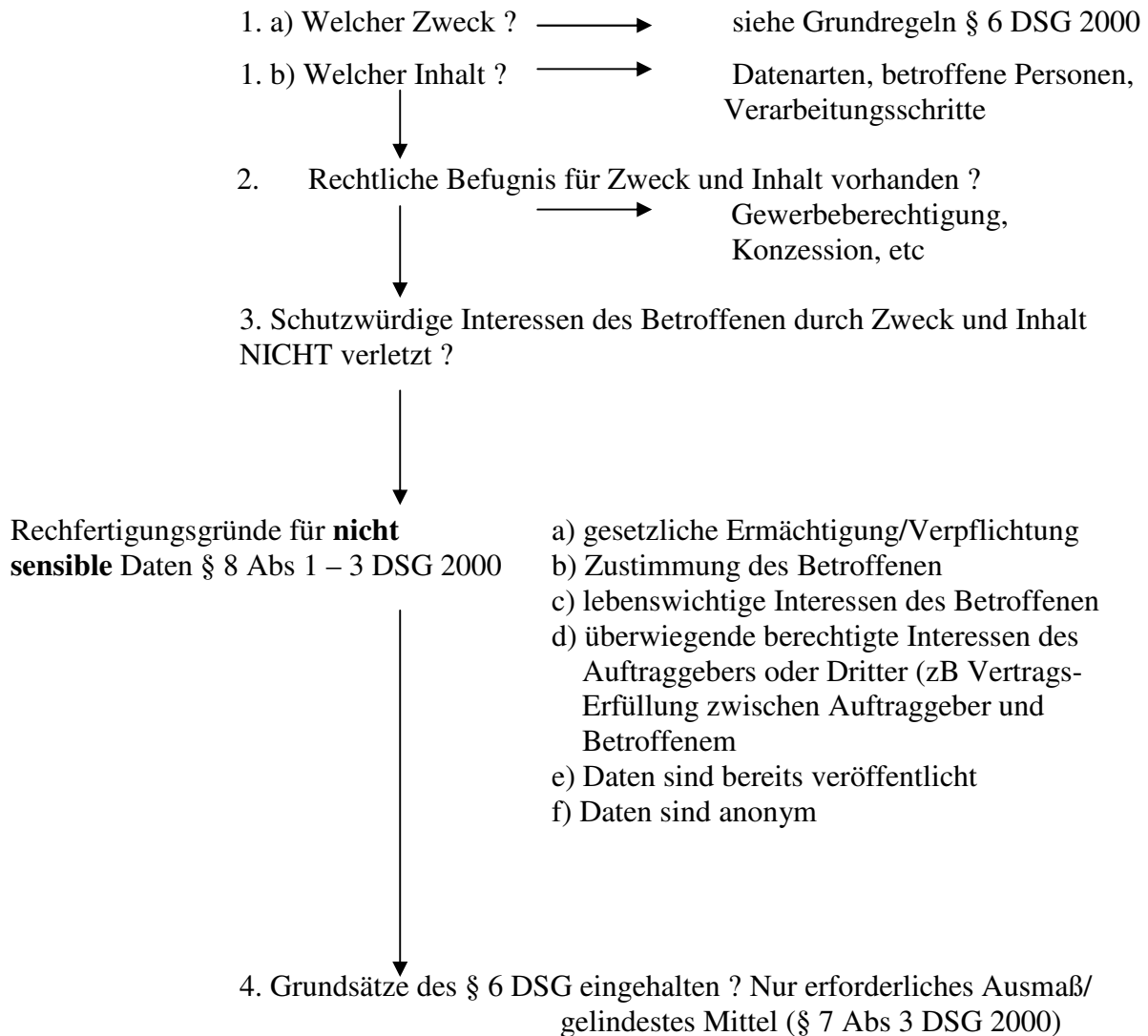
²⁸⁶ *Duschanek/Fischer-Szilagyi* ua, Datenschutzrecht im Unternehmen, 85

Somit ergibt sich abschließend folgendes Prüfungsschema für die Zulässigkeit einer Datenverwendung:

I. Datenverarbeitung ist prinzipiell verboten ! (§ 7 Abs 1 DSG 2000)



II. Ausnahmen von diesem Verbot ? (§ 7 Abs 1 DSG 2000)



III. Datenübermittlung nach § 7 Abs 2 zulässig ?



1. Stammen die Daten aus einer nach § 7 Abs 1 zulässigen Datenverarbeitung ?



2. Was ist der Zweck der Übermittlung ? Hat der Empfänger die rechtliche Befugnis, Daten für diesen Zweck zu verarbeiten ? hat er

diese Befugnis dem Übermittler glaubhaft gemacht ? (§ 7 Abs 2 Z 2 DSG 2000)

- ↓
3. Schutzwürdige Interessen des Betroffenen durch Zweck und Inhalt nicht verletzt ?

Rechtfertigungsgründe für **nicht sensible** Daten (§ 8 Abs 1-3 DSG 2000)

- a) gesetzliche Ermächtigung/Verpflichtung
- b) Zustimmung des Betroffenen
- c) lebenswichtige Interesse des Betroffenen
- d) überwiegende berechnigte Interessen des Auftraggebers oder Dritter zB Vertragserfüllung zwischen Auftraggeber und Betroffenen
- e) Daten sind bereits veröffentlicht
- f) Daten sind anonym

- ↓
4. Grundsätze des § 6 DSG 2000 eingehalten ? Nur erforderliches Ausmaß/gelindestes Mittel ? (§ 7 Abs 3 DSG 2000)

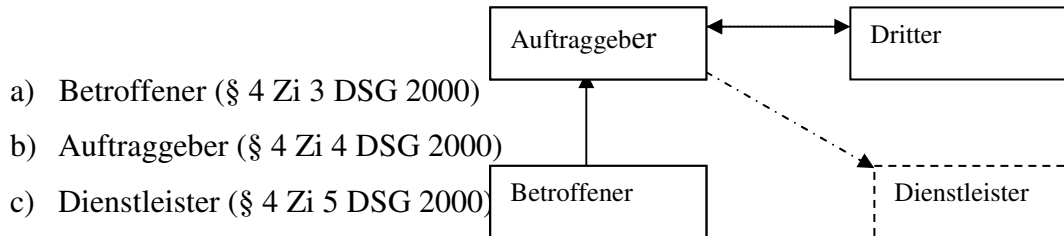
↓

Österreichweite Datenverarbeitung und Datenübermittlung zulässig²⁸⁷

²⁸⁷ Nach *Knyrim*, Datenschutzrecht, 155 ff

7. Die Beteiligten im Datenschutzgesetz

Das Datenschutzgesetz 2000 (DSG 2000) sieht eine Rollenverteilung vor und unterscheidet zwischen



—————> Übermittlung iSd § 4 Z 12 DSG 2000

- - - - -> Überlassung iSd § 4 Z 11 DSG 2000

Die Rollenverteilung zwischen den Akteuren im Datenschutzrecht ist eine diffizile Angelegenheit und hat die einschlägige Literatur im von Anbeginn an immer wieder beschäftigt.

7.1. Der Betroffene („Grundrechtsträger“)

ist jeder vom Auftraggeber (siehe b) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren (personenbezogenen) Daten verwendet werden. Ein darüber hinausgehender Schutzzweck ist aus dem DSG 2000 nicht zu entnehmen.²⁸⁸

Die Verwendung von Daten umfasst einerseits

- die Verarbeitung im Sinne des § 7 Abs. 1 DSG 2000 als auch
- die Übermittlung im Sinne des § 7 Abs. 2 DSG 2000.

Ob es sich dabei um einen In- oder Ausländer handelt spielt keine Rolle. Wenn ein Dritter (z.B. Lieferant, Kunde) Daten über ein Unternehmen benützt, so ist das Unternehmen ebenfalls ein Betroffener.

²⁸⁸ OGH 29.6.2006 6 Ob A 1/06z

Die DS-RL beschränkt sich zwar auf Regelungen zugunsten des Datenschutzes natürlicher Personen (Art 2 lit a DS-RL), lässt aber nationale Rechtsvorschriften zum Schutz juristischer Personen unberührt (Erwägungsgrund 24). Datenschutzinteressen juristischer Personen sind allerdings in der RL 2002/58/EG²⁸⁹ für den Bereich der elektronischen Kommunikation ausdrücklich anerkannt.²⁹⁰

7.2. Der Auftraggeber („Grundrechtsverpflichtete“)

nach § 4 Z 4 DSG 2000 und damit Träger der wesentlichen Pflichten nach dem DSG 2000 – sind natürlich und juristische Personen, Personengemeinschaften (zB OHG, KG, GesnBR) oder wenn sie in Form des öffentlichen Rechts eingerichtet²⁹¹ sind insbesondere Organe einer Gebietskörperschaft oder Geschäftsapparate solcher Organe. Dazu zählen

- Bezirkverwaltungsbehörden
- Landeshauptmann
- (Amt der) Landesregierung
- Minister
- Sozialversicherungsträger
- Kammern

Oder wenn sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind in Form von Beleihungen und Ausgliederungen²⁹² wie zB

- Austro Control Gmbh
- RTR Gmbh
- Telekom Control Gmbh
- ASFINAG
- Unternehmen zur Parkraumüberwachung
- Kfz Begutachter wenn sie in Vollziehung der Gesetze tätig sind

²⁸⁹ Vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl 2002 L 201/37

²⁹⁰ Bernsdorff in Meyer (Hrsg), Kommentar zur Charta der Grundrechte der Europäischen Union, 2003, Art 8

²⁹¹ Umfasst seit dem DSG 2000 nun auch anerkannte Religionsgemeinschaften iSd § 5 Abs 2 Z 1 DSG 2000

²⁹² Die ErläutRV 1613 BlgNR XX. GP erwähnen unter Hinweis auf Art 23 B-VG die Erfassung auch der sog. „schlichten Hoheitsverwaltung“; vgl. dazu auch Jahnel, Datenschutzrecht, 249; Kucsko-Stadlmayer, Art 23 B-VG, Rz 19 mit zahlreichen Fallbeispielen; Schragel, Kommentar zum AHG³, 2003, § 1 AHG, Rz 55ff

wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Wer innerhalb eines Unternehmens für die Datenanwendung verantwortlich ist, ist ohne Belang. Vorstände, Geschäftsführer, Prokuristen und Mitarbeiter entscheiden nämlich über die Verarbeitung von Daten nicht für sich persönlich, sondern in Vertretung und mit Wirkung für die jeweilige juristische Person oder Personengemeinschaft. Das einzelne Organ (nicht im Sinne von „Organ“ einer Gebietskörperschaft) oder einzelner Mitarbeiter kann daher nicht Auftraggeber iSd des DSG 2000 sein.²⁹³ In den Fällen jedoch, in denen der (zivilrechtliche) Auftragnehmer die Vornahme der Datenverarbeitung eigenverantwortlich zu regeln hat (zB Rechtsanwälte, Wirtschaftstreuhänder, Ziviltechniker), wird die Auftraggeberfunktion auf den Erbringer des Werkes verlagert, wenn dies in Rechtsvorschriften, Standes- oder Verhaltensregeln vorgesehen ist. (§ 4 Z 4 letzter Satz DSG 2000)²⁹⁴

Grundsätzlich kann gesagt werden, dass daher meist jener Auftraggeber ist, der personenbezogene Daten eigenverantwortlich verarbeitet. Dies ist wichtig, weil an die Auftraggebereigenschaft auch einige Rechtsfolgen des DSG 2000 anknüpfen: Der Auftraggeber ist verantwortlich für die Einhaltung der Zulässigkeitsvoraussetzungen einer Datenverarbeitung (§§ 6 und 7 DSG 2000), die Einhaltung des schutzwürdigen Geheimhaltungsinteresses (§§ 8 und 9 DSG 2000), für die Meldepflicht der Datenanwendung § 17 DSG 2000) oder die Informationspflicht (§ 24 DSG 2000), die Offenlegungspflicht (§ 25 DSG 2000) sowie die Pflicht zur Richtigstellung und Löschung von Daten iSd § 27 DSG 2000.²⁹⁵

Weiter gilt es zu beachten, dass die Rollenverteilung zwischen Auftraggeber und Dienstleister sich keineswegs mit den entsprechenden Begriffen bzw. Funktionen zivilrechtlicher Rechtsverhältnisse deckt. Ein Auftragsvertrag iSd § 1002ff ABGB wird nicht in Betracht kommen, weil er nur für die Vornahme von Rechtsgeschäften oder anderen Rechtshandlungen für einen anderen zum Inhalt hat. Die Durchführung tatsächlicher Verrichtungen für einen anderen entspricht anderen Vertragsmuster – insbesondere iSd § 1065ff ABGB einem Werkvertrag. Es kommt somit zu einem Auseinanderklaffen von datenschutzrechtlichen und zivilrechtlichen termini.

²⁹³ Duschaneck, DSG 2000, 28

²⁹⁴ Jahnel, Das Datenschutzgesetz 2000. Wichtige Neuerungen, Wbl 02/2000, 49ff

²⁹⁵ Jahnel-Siegrwart-Fercher, Aktuelle Fragen des Datenschutzrechts, 7; Jahnel, Datenschutzrecht, 15

Checkliste – Pflichten des Auftraggebers (im privaten Bereich)²⁹⁶

- Prüfung der Zulässigkeit der Ermittlung (§ 6 DSG 2000)
- Prüfung der Zulässigkeit der Verwendung (§ 7 DSG 2000 ff)
- Datensicherheitsmaßnahmen (§ 14 DSG 2000)
- Belehrung der Mitarbeiter über Datenschutzpflichten (§ 14 Abs 2 Z 3 DSG 2000)
- Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 15 DSG 2000)
- Registrierung (§ 16 DSG 2000 ff)
- Auskunftserteilung (§ 26 DSG 2000)
- Richtigstellung oder Löschung von Daten (§ 27 DSG 2000)
- Angabe der Registrierungsnummer bei Übermittlung und bei Mitteilungen an den Betroffenen (§ 25 Abs 1 DSG 2000)
- Kontrolle des Dienstleisters (§ 10 DSG 2000)

7.3. Der Dienstleister

ist eine natürliche oder juristische Person, Personengemeinschaft oder Organ einer Gebietskörperschaft bzw. deren Geschäftsapparate, wenn sie Daten die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden.²⁹⁷ Hierbei handelt es sich nicht um eine Übermittlung zwischen Auftraggeber und Dienstleister. Der Gesetzgeber geht davon aus, dass zwischen Auftraggeber und Dienstleister zivilrechtlich ein Werkvertrag vorliegt. Dies kann einerseits die Verarbeitung von Daten als Hauptleistung zum Gegenstand haben („einen anderen heranziehen“) oder auch nur ein Nebenprodukt eines auf eine beliebige andere Werkleistung gerichteten Vertrages sein.²⁹⁸ Der Gebrauch der Worte „Auftraggeber“ und „Dienstleister“ kommt jedoch nicht in der Werkvertragsterminologie des ABGB (§§ 1151, 1165 ff) vor und lässt daher den Schluss zu, dass der Gesetzgeber nicht nur ausschließlich Werkverträge im Sinne des ABGB zulassen wollte, sondern den Begriff des „Werkes“ weiter zu verstehen haben will. Darunter fallen ebenso die Besorgung von Aufträgen, Vollmachten, Ermächtigungen.²⁹⁹ Ob das Werk entgeltlich oder unentgeltlich hergestellt wird, ist kein entscheidendes Kriterium.

²⁹⁶ Wittmann [Dr. Arthur Winter], Datenschutzrecht im Unternehmen, 21ff

²⁹⁷ Vgl §§ 4 Z 5 DSG 2000 sowie 10 DSG 2000

²⁹⁸ GZ K121.217/0021-DSK/2006 vom 13.12.2006

²⁹⁹ Zur zivilrechtlichen Abgrenzung vgl. Koziol/Welser II, Bürgerliches Recht, 12. Aufl., 195ff

Jedoch nicht jede beliebige Vertragsgestaltung welche mit einer Datenweitergabe verbunden ist, muss ein Dienstleistungsverhältnis begründen. Die Verfügungsgewalt über die Daten muss vertraglich so geregelt sein, dass ein Vertragspartner (der Dienstleister) an die Verfügungen des anderen Vertragspartners (des Auftraggebers), insbesondere von Richtigstellungen und Löschungen der betreffenden Daten, gebunden ist. Zulässige Verarbeiter werden zunächst jene Unternehmen sein, die über eine Gewerbeberechtigung iSd § 153 GewO für Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik verfügen oder bei anderen Verarbeitern wenn die Eintragung in das Datenverarbeitungsregister (DVR) erfolgt und damit die Zulässigkeit der Aufnahme der Verarbeitungen vom Kreis der Auftraggeber abhängt (etwa im Rahmen von Konzernunternehmen).³⁰⁰ Auch geht die DSK davon aus, dass eine Dienstleistung dann vorliegt, wenn es dem Auftraggeber um das spezielle EDV know-how des Beauftragten geht andernfalls dieser nicht herangezogen wird wenn er keine EDV einsetzt. In der Praxis liegt ein Dienstleister nur dann vor wenn er ein eigenes, rechtlich ausgelagertes Rechenzentrum besitzt.

Damit Daten an einen Dienstleister überhaupt überlassen werden können sind folgende Voraussetzungen notwendig:

- Zweck und Inhalt muss vom Auftraggeber festgelegt worden sein
- der Auftraggeber muss über die rechtliche Befugnis für eine derartige Datenverarbeitung verfügen
- es dürfen keine schutzwürdigen Geheimhaltungsinteressen des/der Betroffenen verletzt sein

Dies wird vor allem dann nicht der Fall sein wenn

- der Betroffene der Datenverarbeitung zugestimmt hat,
- dies zur Erfüllung eines Vertragsverhältnisses mit dem Betroffenen notwendig ist oder
- der Auftraggeber gesetzliche Pflichten erfüllt

³⁰⁰ ÖZW 1979/1, 17

Wenn diese Kriterien erfüllt sind, dann kann der Auftraggeber die Daten dem Dienstleister überlassen, soweit dieser auch noch die Kriterien nach §§ 10 und 11 DSG 2000 erfüllt.

Der datenschutzrechtliche Dienstleisterbegriff bedarf einer genauen Abgrenzung vom Auftraggeberbegriff da für diesen eine eingeschränkte datenschutzrechtliche Verantwortung besteht. (§ 11 DSG 2000). Die Verantwortung im Außenverhältnis gegenüber dem Betroffenen, d.h. die Beachtung der rechtmäßigen Er- und Übermittlung, Auskunftserteilung, Berichtigung und Löschung von unrichtigen Daten, verbleibt beim Auftraggeber. Laut übereinstimmender Lehre beschränkt sich der Dienstleisterbegriff auf Fälle von Rechenzentrumsdienstleistungen³⁰¹ wenn das Schwergewicht auf den Einsatz der EDV gerichtet ist und die Verwendung dieser eine direkte Folge der Aufnahme der Datenverarbeitung ist. Zu beachten ist jedoch weiters, dass eine Auftragserteilung an Ärzte, Rechtsanwälte, Inkassobüros, Auskunftsteien, Immobilienreuhänder, Adressverlage, Ziviltechniker etc idR kein Dienstleistungsverhältnis begründet. Erhalten diese zur Geschäftsabwicklung Daten vom Kunden, so sind diese als Auftraggeber mit allen datenschutzrechtlichen Pflichten zu qualifizieren.

Voraussetzung für die Qualifikation als Dienstleister nach § 4 Z 5 DSG 2000 ist, dass die vom (zivilrechtlichen) Werkbesteller weitergegebenen (oder auch für seine Zwecke vom Werkunternehmer ermittelten) Daten ausschließlich zu diesem Zweck verwendet werden. Werden die Daten hingegen darüber hinaus auch für andere Zwecke - insbesondere Werke anderer Werkbesteller - verwendet, so ist der Verwender Auftraggeber (§ 4 Z 4 leg. cit.). Dies zeigen auch die in den erläuternden Bemerkungen zu § 4 Z 4 und 5 DSG 2000³⁰² zum Ausdruck kommenden Rechtsschutzaspekte: Wenn bei einem Werkunternehmer die Daten nicht nur für Zwecke der Herstellung eines Werks verwendet werden, kann nicht von entscheidungswesentlichen Verfügungsrechten der Werkbesteller an den Daten ausgegangen werden, dh sie können jedenfalls keine vollständige Löschung der Daten beim Werkunternehmer erreichen. Ein Zugänglichmachen von Datenanwendungen über ein Portal, das von einem anderen Rechtsträger als dem Auftraggeber der Datenanwendung betrieben ist („das Werk“), ist der Portalbetreiber als Dienstleister anzusehen sofern er auf den Inhalt der Datenanwendung keinen Einfluss hat. Ein Entgelt an den Portalbetreiber zur Benützung ist

³⁰¹ Duschaneck, DSG 2000, 24

³⁰² ErläutRV 1613 BlgNR XX. GP

kein eindeutiges Indiz, dass der Portalbetreiber die Rolle eines Auftraggebers übernommen hat.³⁰³

Doch ist auch hier äußerste Vorsicht geboten, da die Akteure während des Geschehens ihre rechtliche Position (wenn auch nicht freiwillig) ändern können. So wird ein (ehemaliger) Mitarbeiter der Finanz- oder Kundendaten (Wirtschaftsdaten eines Unternehmens bzw. dessen eigene Geschäfts- und Betriebsgeheimnisse fallen nach hL und stRsp unter das DSG)³⁰⁴ eines Unternehmens (illegaler weise) mitnimmt, zum Auftraggeber iSd § 4 Z 3 DSG 2000 wenn er sich entschließt diese zum eigenen Zweck zum verarbeiten und der (ehemalige) Arbeitgeber zum Betroffenen. Im Verhältnis zum Kunden/Lieferanten werden diese Betroffene und der ehemalige Mitarbeiter wiederum Auftraggeber. *Singer* führt in seinem Beitrag im Buch „Datenschutzrecht im Unternehmen“³⁰⁵ ganz richtig an Hand eines plastischen Beispiels aus, dass es datenrechtlich irrelevant ist, ob jemand (egal ob Einzelperson oder juristische Person) über sich selbst in *seinem* Computer zB Daten über eine eigene Krankheit oder seine unternehmerischen Misserfolge verarbeitet. Erhält diese Daten aber sodann ein Dritter und verarbeitet diese für seinen eigenen Vorteil (dh neuen Zweck) in *seinem eigenen* Computer weiter, so wird der bisherige „Eigenverarbeiter“ zum „Betroffenen“. Aber noch mehr betroffen wird er sein wenn ihm der OGH nicht als Betroffenen ansieht (weil es ja laut dessen Argumentation seine eigenen Daten sind) und ihm keine Verteidigungs- bzw. Betroffenenrechte zubilligt.

Auch wenn der OGH im Beschluss³⁰⁶ in seiner Argumentation in sich stimmig, aber von einer falschen Schlussfolgerung ausgehend, gegenteiliger Ansicht ist, so macht nur dieser „Rollenwechsel“ im Gesamtkontext des DSG Sinn. Solcher Art Verletzungen von datenschutzrechtlichen Bestimmungen können geeignet sein, einen sachlich nicht gerechtfertigten Vorsprung gegenüber Mitbewerbern zu erlangen, und dies ein sittenwidriges Handeln iSd § 1 UWG bedeutet.³⁰⁷ Desweiteren wird durch diese Handlung § 7 Abs 2 DSG 2000 (unrechtmäßige Datenübermittlung) als auch § 15 DSG 2000 (Datengeheimnis) verletzt. Hier ist weiters auf die Strafbestimmung des § 51 DSG 2000 hinzuweisen, die vorsieht, dass mit Freiheitsstrafen bis zu einem Jahr zu bestrafen ist, wer in der Absicht, sich einen Vermögensvorteil zu verschaffen, personenbezogene Daten benützt, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder

³⁰³ K121.155/0015-DSK/2006

³⁰⁴ VfSlg 12.228/1989; *Duschanek*, Der Umfang des Begriffes „personenbezogene Daten“ im DSG, in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, 60

³⁰⁵ *Wittmann*, Datenschutzrecht im Unternehmen (1991), ...

³⁰⁶ OGH 4. 5.2004, 4 Ob 50/04

³⁰⁷ *Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004/55, 870

die er sich widerrechtlich verschafft hat, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat. § 11 UWG welcher nur während eines aufrechten Beschäftigungsverhältnisses vor Konkurrenz schützt, würde jedoch einer Anwendung der Strafbestimmungen des DSG 2000 nicht im Wege stehen.³⁰⁸

In einer Vorstellung gegen den Mandatsbescheid der DSK zur Untersagung des Betreibens eines Kreditinformationssystems³⁰⁹ wurden die Begriffe „Auftraggeber“ und „Dienstleister“ nochmals eindeutig festgelegt. Darin betrieb ein Telekommunikationsunternehmen ein über das Internet zugängliches Kreditinformationssystem welches mit Daten einer Wirtschaftsauskunftei hinterlegt ist aber entgegen den Bestimmungen der § 17 Abs 1 und § 18 Abs 2 Z 3 DSG 2000 nicht vorab von der DSK genehmigt wurde. Obwohl argumentiert werden kann, dass die Telekomgesellschaft bei der Herstellung der Verbindung zwischen Wirtschaftsauskunftei und Kunden Daten zwischenspeichert, so belegt ein sodann vorgelegter abgeschlossener Vertrag zwischen Telekomgesellschaft und Wirtschaftsauskunftei, dass nicht sie Auftraggeber iSd § 4 Z 4 DSG 2000 ist sondern die Wirtschaftsauskunftei die rechtlichen, systemtechnischen, organisatorischen und finanziellen Aspekte des Datenaustausches organisiert und entscheidet. Diese Entscheidungsbefugnis legitimiert die Kreditauskunftei zum Auftraggeber mit all seinen rechtlichen Pflichten und das Telekommunikationsunternehmen zum „bloßen“ Vertriebspartner und Dienstleister.

Die Unterscheidung ob ein Dienstleisterverhältnis vorliegt oder nicht, ist sehr wichtig weil wenn Daten von einem Auftraggeber an einen Dienstleister weitergegeben werden, die strengen Voraussetzungen des § 7 Abs 2 DSG 2000 (siehe Kapitel 6.3.) nicht erfüllt sein müssen. Denn es handelt sich in diesem Fall nicht um eine Übermittlung iSd § 7 Abs 2 DSG 2000 sondern um eine bloße „Überlassung“. Weiters darf auf die Dienstleistervereinbarung³¹⁰ gemäß §§ 10 und 11 DSG 2000 (welcher aus Gründen der Beweisbarkeit am besten schriftlich abgeschlossen werden sollte) nicht vergessen werden.

Auf Webseiten, die nur als Dienstleistung für Dritte betrieben werden, muss entsprechend §§ 25 Abs 1 und 24 Abs 2 DSG 2000 offen gelegt werden wer datenschutzrechtlicher Auftraggeber ist um somit Irrmeinungen und falsche Adressaten vorweg zu vermeiden.

Aufgrund der dem Dienstleister vorgeschriebenen Datensicherheitsmaßnahmen des § 14 DSG 2000 wird von diesem auch ausdrücklich verlangt, dass seine Mitarbeiter zur Einhaltung des

³⁰⁸ *Jahnel*, OGH: Kein Schutz von Unternehmensdaten nach dem DSG ?, RdW 2005/244, 200ff; *Knyrim*, *ecolex* 2004, 874; Dohr-Pollirer-Weiss², *Datenschutzrecht*, E 5 zu § 4

³⁰⁹ GZ K211.489/008-DSK/2003 vom 11.7.2003; *Knyrim*, *ecolex* 2004, 71, 414

³¹⁰ Zu weiteren Details des Dienstleistervertrages kann hier nicht extra eingegangen werden

Datengeheimnisses iSd § 15 DSG 2000 verpflichtet werden. Dies ist jedoch nicht notwendig wenn sie ohnehin einer gesetzlichen Verschwiegenheitspflicht unterliegen (zB dem Bankgeheimnis aufgrund § 38 BWG oder der anwaltlichen Schweigepflicht der §§ 8 und 9 RAO). Unterliegt der Auftraggeber besonderen Verschwiegenheitspflichten, so muss er den Dienstleister bzw. dessen Mitarbeiter ebenfalls vertraglich extra dazu verpflichten. Dazu ist eine ausdrückliche und schriftliche vertragliche Regelung notwendig, denn eine solche Überantwortung erfolgt nicht von Gesetz wegen durch § 11 DSG 2000.³¹¹

³¹¹ *Duschanek/Rosenmayr-Klemenz*, DSG, 56; *Knyrim*, Datenschutzrecht, 197

Zusammengefasst hat der Dienstleister folgende Pflichten:

- Die Daten dürfen ausschließlich im Rahmen der Aufträge des Auftraggebers verwendet werden. Die Übermittlung ohne Auftrag des Auftraggebers ist verboten.
- Sowohl für den Dienstleister als auch den Auftraggeber besteht die Pflicht Datensicherheitsmaßnahmen zu treffen. (Zutrittskontrollen, Absicherung der EDV hardware,...). Weiters besteht die Pflicht iSd § 14 DSG 2000 Protokoll³¹² zu führen um Verwendungsvorgänge nachvollziehen zu können. Der Aufbau der Datensicherung ist prinzipiell die Aufgabe des Arbeitgebers.³¹³ Für den beauftragten Arbeitnehmer besteht Weisungspflicht.
Als Mitarbeiter darf nur herangezogen werden, wer sich dem Dienstleister bzw. dem Auftraggeber gegenüber zur Einhaltung des Datengeheimnisses iSd § 15 DSG 2000 verpflichtet hat oder soundso einer gesetzlichen Verschwiegenheitspflicht unterliegt.
- Weitere Dienstleister dürfen nur mit Genehmigung des Auftraggebers herangezogen werden.
- Im Einvernehmen mit dem Auftraggeber müssen alle notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunft-, Richtigstellungs- und Löschungspflicht des Auftraggebers geschaffen werden.
- Nach Beendigung des (Dienstleistungs-)Auftrages sind alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in den dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten.
- Dem Auftraggeber sind jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der oben genannten Verpflichtungen notwendig sind

³¹² Wobei zu beachten ist, dass dieses Protokoll wieder in einer Datei mit personenbezogenen Daten gespeichert ist und das DSG seine Anwendung findet.....

³¹³ OGH 29.8.1990, 9 Ob A 182/90 = RdW 1991,87

8. Das EuGH Urteil im Fall „Lindqvist“

Da zB der KSV und auch andere Wirtschaftsauskunfteien sämtliche Datenbankabfragen „online“ mittels Internet Zugriff ermöglicht, stellt sich schon vorab die Frage ob der Zulässigkeit der Veröffentlichung von personenbezogenen Daten im Internet. Ich ziehe hierzu das Vorabentscheidungsverfahren Rs C-101/01 Lindqvist, EuGH 6.11.2003, heran worin die Frage beantwortet wurde ob es sich beim „veröffentlichen“ um eine Verarbeitung iSd DS-RL 95/46EG handelt und ob diese zulässig sei obwohl der EuGH diesbezüglich eine strenge Auslegung der DS-RL 95/46/EG vertritt.

Der EuGH meinte dazu, dass *„die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise [...] erkennbar zu machen, eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten im Sinne von Art 3 Abs 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz personenbezogener Daten und zum freien Datenverkehr darstellt.“*³¹⁴

- Informationen über Personen ins Internet zu stellen und diese anhand von genauen persönlichen Daten identifizierbar zu machen, stellt eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten iSd Art 3 Abs 1 sowie Art 7 und 8 (für besondere Kategorien von Daten) der DS-RL dar und § 7 Abs 2 iVm § 8 bzw. 9 DSG 2000 [für sensible Daten] geregelten Voraussetzungen erfüllen muss, um zulässig zu sein.

- Eine solche Verarbeitung fällt nicht unter eine in Art 3 Abs 2 genannten Ausnahmen. Unter diesen Ausnahmen wird die Verwendung im persönlichen bzw. familiären Bereich verstanden.

- Es liegt jedoch keine Übermittlung von Daten in ein Drittland iSd Art 25 der DS-RL vor, wenn eine in einem Mitgliedsstaat aufhältige Person, eine Internetseite im selben Mitgliedsstaat oder einem anderen Mitgliedsstaat unterhält wo personenbezogene Daten von ansässigen natürlichen oder juristischen Person gespeichert sind, diese Seite von jeder Person welche eine Verbindung zum Internet herstellt abgerufen werden kann, einschließlich Personen in Drittländern, zugänglich macht.³¹⁵ Es handelt sich hierbei um ein „abrufbar

³¹⁴ EuGH Rs C-101/01, Lindqvist, Slg 2003, I-12971, Rn 27

³¹⁵ Hörlsberger, Veröffentlichung personenbezogener Daten im Internet, ÖJZ 2004/45

machen“ und damit um eine Übermittlung von Daten iSd § 4 Z 12 SG 2000. Für die Voraussetzungen für die Zulässigkeit siehe oben.

- Liegen diese Voraussetzungen vor, so handelt es sich immer um zulässigerweise veröffentlichte Daten, die sodann wiederum genehmigungsfrei für eine Übermittlung ins Ausland iSd § 12 Abs 3 bzw Abs 5 2000 sind. (Die DS-RL spricht auch von „verbreiten“ und regelt Näheres bei der „Verarbeitung von Daten“[siehe Kapitel 6.]; dies darf nur dann erfolgen wenn die sechs Voraussetzungen des Art 7 DS-RL [siehe Anhang II] erfüllt sind)

- Art 26 Abs 1 lit f lässt die Übermittlung von „Registern“ zu, die „gemäß den Rechts- und Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt sind und entweder der gesamten Öffentlichkeit oder bestimmten Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen....“ . Diese Regelung stellt auf das Grundbuch, das Handelsregister und diverse Schuldnerlisten ab.³¹⁶ Wobei unter dem Begriff „Register“ im weitesten Sinn, das gesamte Internet subsumiert werden kann.

- Es gibt zwar in Österreich keine Rechts- und/oder Verwaltungsvorschriften, die ausdrücklich besagen, dass das Internet zur Information der Öffentlichkeit dient,³¹⁷ aber dies ist auch eigentlich nicht erforderlich weil sich der Zweck bei von Privatpersonen betriebenen Registern aus deren Widmung ergibt. Das ein solches „Register“ dem öffentlichen Bereich (von einer staatlichen Stelle betrieben wird) angehören muss, wird in der DS-Richtlinie nicht vorausgesetzt.³¹⁸ Bei extensiver Auslegung des Art 26 der DS-RL sind somit § 12ff DSG 2000 richtlinienkonform zu interpretieren.

³¹⁶ *Dammann/Simitis*, EG-Datenschutzrichtlinie, (FN 8) Art 26 Rz 11

³¹⁷ Ausgenommen § 24 ECG welches von „Veröffentlichen“ im Internet spricht

³¹⁸ *Hörlsberger*, ÖJZ 2004,45; *Ehmann/Helfrich*, EG DS-RL, Art 26, Rz 15 iVm Art 18 Rz 23

9. Das EuGH Urteil im Fall „Asnef-Equifax/Ausbanc“

Sollte bis dato die Existenz von der Führung einer Kreditevidenz von Verbraucher-, Kartell- und Datenschützern in Frage gestellt worden sein, so ist (zumindestens) auf europäischer Ebene die Existenz einer solchen in Bezug auf Behinderung des Wettbewerbs, neben jener der jeweiligen Nationalbank obliegenden Führung, seit dem Urteil EuGH 23.11.2006, C-238-05³¹⁹ geklärt.

Darin wollte die spanische Gesellschaft der Nutzer von Bankdienstleistung („Asociacion de Usuarios des Servicios Bancarios - kurz „Ausbanc“) einer anderen Gesellschaft („Asnef-Equifax, Servicios de Informacion sobre Solvencia y Credito“- kurz „Asnef-Equifax“) sowie der „Administracion del Estado“ den Aufbau eines (weiteren) Kreditinformationssystem zwischen Finanzinstituten bezüglich der Zahlungsfähigkeit von Kunden mit Verweis auf das spanische Kartell- (welches fast ident ist mit den Regeln des Art 81 Abs und 3 EG) und Wettbewerbsrecht zu untersagen. Begründet wurde dies mit der Behinderung des freien Wettbewerbs da es einen Austausch von Auskünften voraussetze die unter Wettbewerbern generell als Geschäftsgeheimnisse gelten und wodurch Risikofaktoren, die mit jeder Unternehmensentscheidung verbunden seien, ausgeschlossen würden und gleichförmige Reaktionen der Finanzinstitute gegenüber Kreditantragstellern gefördert würden und es könne daher nicht nach den Ausnahmen des Art 3 (nationales Recht) genehmigt werden.

Zur Frage der Vorabentscheidung kam es ob dieses Register ungünstige Auswirkungen auf die Wirtschaftspolitik der Union und auf den Kreditmarkt der Gemeinschaft sowie eine Beschränkung des Wettbewerbs im Bereich der Finanz- und Kreditinstitute bewirke und ob eine Zulässigkeit der Einrichtungen eines Kreditauskunftsregisters mit dem Nutzen für Verbraucher begründet werden kann. Prinzipiell ist es daher auch nicht auszuschließen, dass ein und derselbe Sachverhalt sowohl unter das gemeinschaftliche als auch unter das nationale Wettbewerbsrecht fällt, auch wenn diese Rechtsordnungen die betreffenden Verhaltensweisen unter unterschiedlichen Gesichtspunkten würdigen.³²⁰

³¹⁹ CELEX-Nummer: 62005J0238; *Koziol*, ÖBA 2007/27 (EuGH)

³²⁰ Vgl. in diesem Sinne Urteil vom 26.11.1998 in der Rs CS-7/97, *Bronner*, Slg 1998,I-7791, Rn 19

Art 81 Abs 1 EG³²¹ ist dahin auszulegen, dass ein System zum Austausch von Kreditinformationen zwischen Finanzinstituten grundsätzlich keine Beschränkung des Wettbewerbs im Sinne dieser Bestimmung bewirkt, sofern der betroffene Markt oder die betroffenen Märkte nicht hochgradig konzentriert sind, dieses System keine Identifikation der Gläubiger ermöglicht und die Zugangs- und Nutzungsbedingungen für die Finanzinstitute rechtlich und tatsächlich keine Diskriminierung enthalten. Beschränkt ein System zum Austausch von Kreditinformationen den Wettbewerb im Sinne des Art 81 Abs 1 EG, so hängt die Anwendbarkeit der Ausnahme des Art 81 Abs 3 EG von der kumulativen Erfüllung der dort genannten vier Tatbestandsmerkmale ab.

Für die Erfüllung des Tatbestandsmerkmals, dass der Verbraucher an dem entstehenden Gewinn angemessen beteiligt wird, ist es grundsätzlich nicht erforderlich, dass jeder einzelne Verbraucher einen Nutzen zieht. Vielmehr muss die Auswirkung auf die Verbraucher auf den relevanten Märkten insgesamt günstig sein. Nachdem das „neue“ Kreditinformation grundsätzlich allen im Kreditwesen tätigen Instituten zur Verfügung steht und im Vergleich zu jenem von der spanischen Zentralbank geführten keine Mindestbeträge vorgesehen werden, wird diese eine dementsprechende größere Anzahl von Kreditvorgängen betreffen. Gleichzeitig werden die Auskünfte aus diesem Register durch EDV bearbeitet und übermittelt und sind somit schneller verfü- und greifbar. Dadurch ist die Möglichkeit des Zugangs zu

³²¹ Art 81 EG lautet: *(1) Mit dem Gemeinsamen Markt unvereinbar und verboten sind alle Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, welche den Handel zwischen Mitgliedstaaten zu beeinträchtigen geeignet sind und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des Gemeinsamen Marktes bezwecken oder bewirken, insbesondere*

- a) die unmittelbare oder mittelbare Festsetzung der An- oder Verkaufspreise oder sonstiger Geschäftsbedingungen;*
- b) die Einschränkung oder Kontrolle der Erzeugung, des Absatzes, der technischen Entwicklung oder der Investitionen;*
- c) die Aufteilung der Märkte oder Versorgungsquellen;*
- d) die Anwendung unterschiedlicher Bedingungen bei gleichwertigen Leistungen gegenüber Handelspartnern, wodurch diese im Wettbewerb benachteiligt werden;*
- e) die an den Abschluss von Verträgen geknüpfte Bedingung, dass die Vertragspartner zusätzliche Leistungen annehmen, die weder sachlich noch nach Handelsbrauch in Beziehung zum Vertragsgegenstand stehen.*

(2) Die nach diesem Artikel verbotenen Vereinbarungen oder Beschlüsse sind nichtig.

(3) Die Bestimmungen des Absatzes 1 können für nicht anwendbar erklärt werden auf

- Vereinbarungen oder Gruppen von Vereinbarungen zwischen Unternehmen,*
- Beschlüsse oder Gruppen von Beschlüssen von Unternehmensvereinigungen,*
- aufeinander abgestimmte Verhaltensweisen oder Gruppen von solchen,*

die unter angemessener Beteiligung der Verbraucher an dem entstehenden Gewinn zur Verbesserung der Warenerzeugung oder -verteilung oder zur Förderung des technischen oder wirtschaftlichen Fortschritts beitragen, ohne dass den beteiligten Unternehmen

- a) Beschränkungen auferlegt werden, die für die Verwirklichung dieser Ziele nicht unerlässlich sind, oder*
- b) Möglichkeiten eröffnet werden, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten.*

diesem Register von allen in Spanien tätigen oder beabsichtigt tätig zu werdenden Unternehmen von erheblicher Bedeutung.

Solche Register gibt es in vielen Staaten und sie verbessern die Kenntnisse der Kreditinstitute über potentielle Kreditnehmer indem sie die Ungleichheit des Informationsstandes zwischen Gläubiger und Schuldner verringern und dadurch die Rückzahlungswahrscheinlichkeit erhöhen. Dadurch sind diese Register grundsätzlich geeignet, die Ausfallsquote von Kreditnehmern zu verringern und den Wirkungsgrad des Kreditangebots zu erhöhen.

Vereinbarungen über den Austausch von Informationen verstoßen nach der einschlägigen Rechtssprechung gegen die Wettbewerbsregeln, wenn sie den Grad der Ungewissheit über das fragliche Marktgeschehen verringern oder beseitigen und dadurch zu einer Beschränkung des Wettbewerbs zwischen den Unternehmen führen.³²² Prinzipiell kann jeder Wirtschaftsteilnehmer selbständig bestimmen, welche Politik er auf dem Gemeinsamen Markt zu betreiben gedenkt. Ein solches Selbständigkeitspostulat steht nach der stRsp jeder unmittelbaren oder mittelbaren Einflussnahme zwischen Wirtschaftsteilnehmern entgegen, durch die entweder das Marktverhalten eines tatsächlichen oder potentiellen Wettbewerbers beeinflusst oder ein solcher über das Marktverhalten ins Bild gesetzt wird. Dieses Selbständigkeitspostulat nimmt jedoch den Wirtschaftsteilnehmern nicht das Recht, sich dem festgestellten oder zu erwartenden Verhalten ihrer Konkurrenten auf intelligente Weise anzupassen.³²³ Solche Register führen dazu, dass sie die Bedeutung der Informationen vermindern die Finanzinstitute über ihre eigenen Kunden zur Verfügung haben, sie erhöhen die Mobilität von Kreditnehmern und erleichtern den Markteintritt neuer Wettbewerber.

Folgende Überlegungen wurden vom EuGH an die Errichtung eines Kreditinformationsregistern gestellt:

1. Im Falle eines „zersplitterten“ Marktes wird die Verbreitung und der Austausch von Informationen unter Wettbewerbern neutrale oder sogar positive Wirkung auf die Wettbewerbssituation des Marktes haben. Im Gegensatz dazu wird bei einer hochgradigen Konzentration des Angebot der Austausch bestimmter Informationen geeignet sein, den Unternehmen Aufschluss über Position und Geschäftsstrategie ihrer Wettbewerber auf dem

³²² EuGH vom 28.5.1998, Rs C-7/95 P Deere/Kommission, Rn 90; EuGH vom 2.10.2003, Rs C-194/99 P, Thyssen Stahl/Kommission, Slg 2003, I-10821, Rn 81

³²³ Vgl. Deere/Kommission, Rn 87; Kommission/Anic Partecipazioni, Rn 117; Thyssen Stahl/Kommission, Rn 83

Markt zu geben wodurch der Wettbewerb auf diesem Markt verfälscht und die Wahrscheinlichkeit eines kollusiven Zusammenwirkens erhöht werden könnte.

2. Die Identität der Gläubiger darf nicht unmittelbar oder mittelbar aufgedeckt werden um die Stellung von Wettbewerbern oder deren Geschäftsstrategie auf dem Markt preiszugeben.

3. Das Register muss allen im maßgeblichen Bereich tätigen Wirtschaftsteilnehmern diskriminierungsfrei zugänglich sein. Wenn dies nicht gewährleistet wird, werden Wirtschaftsteilnehmer die über weniger Informationen zur Einschätzung des Risikos verfügen benachteiligt wodurch der Markteintritt neuer Wirtschaftsteilnehmer erschwert wird.

Wenn all diese Voraussetzungen gegeben sind, ist ein System zum Austausch von Informationen grundsätzlich nicht geeignet, eine Beschränkung des Wettbewerbs iSd Art 81 Abs 1 EG zu bewirken.

Die Anwendbarkeit der Ausnahme des Art 81 Abs 3 EG hängt, wie bereits erwähnt, von der kumulativen Erfüllung von den dort genannten vier Tatbestandsmerkmalen ab:

1. Das Kartell muss zur Verbesserung der Erzeugung oder Verteilung der fraglichen Waren oder Erbringung der fraglichen Dienstleistungen oder zur Förderung des technischen oder wirtschaftlichen Fortschritts beitragen.
2. Der Verbraucher muss an dem entstehenden Gewinn angemessen beteiligt sein
3. Das Kartell darf den beteiligten Unternehmen keine nicht unerlässlichen Beschränkungen auferlegen
4. Dem Kartell darf keine Möglichkeit eröffnet werden, für einen wesentlichen Teil der betreffenden Waren oder Dienstleistungen den Wettbewerb auszuschalten.

Wie bereits festgehalten, sind solche Register geeignet sowohl die Ausfallsquote zu verringern, den Wirkungsgrad des Kreditangebots zu erhöhen, die Mobilität der Kreditnehmer zu erhöhen und auch der Überschuldung von Kreditnehmern vorzubeugen.

Diese wirtschaftlichen Vorteile könnten im Fall einer Beschränkung des Wettbewerbs durch das Register die Nachteile einer solchen Beschränkung aufwiegen wodurch jedoch auch nicht ausgeschlossen werden kann, dass sich bestimmte Kreditantragsteller wegen der Existenz eines solchen Register höheren Zinssätzen oder einer Ablehnung gegenüber stehen. Die günstigen Auswirkungen müssen für die Gesamtheit der Verbraucher auf den relevanten

Märkten eintreten, jedoch aber nicht für jeden einzelnen. Umgekehrt kann dies jedoch auch dazu führen, dass Kreditantragsteller günstigere Zinssätze bekommen weil die Kenntnisse über die Gläubiger verbessert werden.

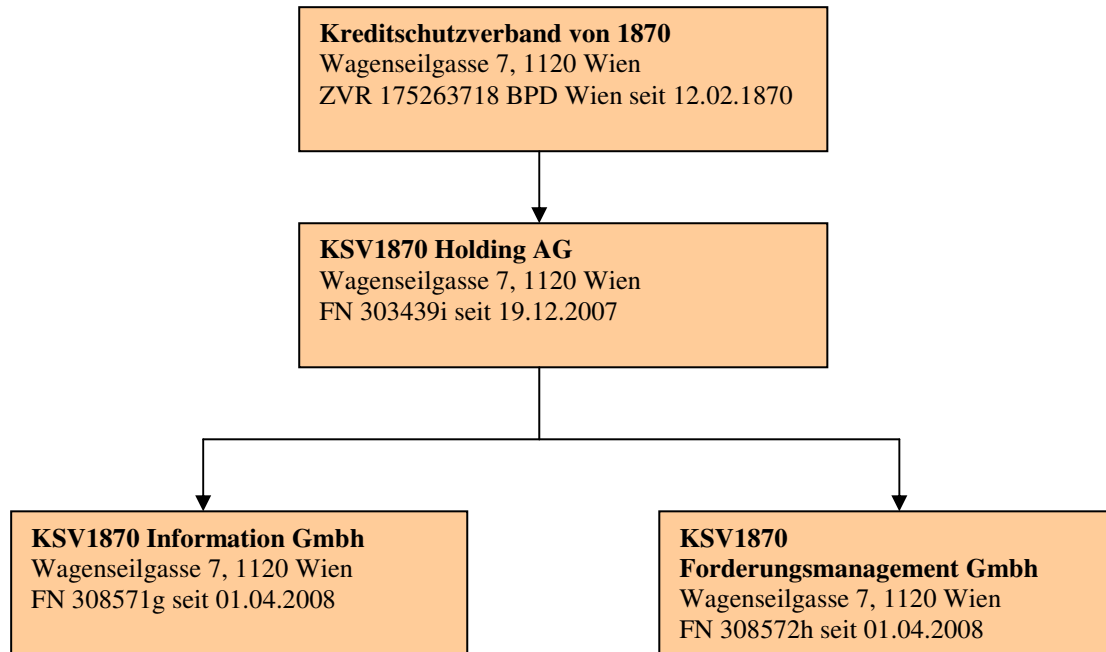
10. Der Kreditschutzverband von 1870 (KSV)

Der Kreditschutzverband besteht in der Rechtsform eines Vereines (ZVR 175263718) seit 1870 in Österreich und gehört den ca. 20.000 freiwilligen Mitgliedern. Der KSV verfügt über insgesamt zwei Gewerbeberichtungen und zwar folgende:

- § 152 GewO Kreditauskunftei
- § 94 Z 36 GewO Inkassoinstitut

Seit neuerdings wurde die Gesellschaftsstruktur geändert und in Form von drei Gesellschaften mit beschränkter Haftung aufgegliedert.

- KSV1870 Holding AG
- KSV1870 Information GmbH
- KSV1870 Forderungsmanagement GmbH



Leistungsdaten KSV 2007

KSV

- 20.000 Mitglieder, 14.500 Online-Kunden mit 24.500 Usern
- Zentrale in Wien, 6 Niederlassungen in den Bundesländern
- 420 Mitarbeiter und Mitarbeiterinnen
- EUR 43 Mio. Umsatz

Umsatzverteilung

- 51 % mit Information
- 29 % mit Inkasso
- 20 % mit Insolvenz

Information

- 5,3 Mio. erteilte Bonitätsauskünfte (Business & Consumer)
- 70 % des Info-Umsatzes über e-Business-Lösungen

Inkasso

- 152.000 übergebene Inkassofälle
- EUR 183 Mio. Gesamtvolumen

Insolvenz

- 10.400 Verfahren (eröffnete Firmen- und Privatkonkurse)
- 31.800 erteilte Aufträge³²⁴

³²⁴ <http://www.ksv.at>

10.1. Die Bonitäts-/Wirtschaftsauskunft im Allgemeinen

Eine Wirtschaftsauskunft kann neben dem direkt Auskunftsbetroffenen (wobei es sich um eine physische oder juristische Person oder um Personengemeinschaften des Handelsrecht handeln kann) auch Angaben über Personen enthalten, die in einer vollständigen Auskunft enthalten sein müssen wie zB Gesellschafter, leitende Organe, im Betrieb tätige Familienangehörige, etc. All diese Personen können als Betroffene im Sinne der datenschutzrechtlichen Bestimmungen in Betracht kommen.

Die Einbeziehung einzelner Angaben zur Persönlichkeit ist für eine objektive Darstellung vielfach unentbehrlich. Um die Aussagekraft über unternehmensbezogene Informationen zu steigern, ist auch das Eingehen auf private Verhältnisse teilweise erforderlich, wenn dies von geschäftlicher Relevanz ist. Angaben über Unterhaltsverpflichtungen, privaten Aufwand, Haftaufenthalte verlieren sodann ihren privaten Charakter, wenn sich daraus Rückschlüsse auf die Eignung zur Unternehmensführung oder Konsequenzen für wirtschaftliche Belastungen des Unternehmens ergeben.³²⁵ Es ist unstreitig, dass für die Beurteilung der Kreditwürdigkeit neben den unmittelbaren Verhältnissen des Unternehmens auch die persönliche Zuverlässigkeit und das Vertrauen in die Fähigkeiten der Unternehmensführung ausschlaggebend sind.³²⁶ Solche Angaben haben Eingang in eine Wirtschaftsauskunft zu finden, wobei auf eventuelle subjektive Beurteilungen oft nicht verzichtet werden kann oder aber auch der geschulte Empfänger der Auskunft sich ein eigenes Bild darüber machen soll.³²⁷

Im Hinblick auf die von der Rechtsordnung anerkannte Tätigkeit gewerblicher Auskunftsteile muss der Wirtschaftstreibende heutzutage rechnen, dass über ihn bzw. das Unternehmen Aufzeichnungen bei den Auskunftsteilen gemacht werden und Auskünfte an Geschäftspartner erteilt werden.

Da die Einholung solcher Auskünfte (insbesondere beim ersten Geschäftsabschluss) mehr die Regel als die Ausnahme darstellt, kann man sie heute wohl zur Sorgfalt eines ordentlichen Kaufmanns iSd § 347 UGB zählen. In dieser Situation wird es idR an einem schutzwürdigen Interesse an der Geheimhaltung der in diesem Bereich fallenden Daten fehlen. Damit wären die tatbestandsmäßigen Voraussetzungen für die Inanspruchnahme des Grundrechts iSd § 1

³²⁵ Tiedemann – Sasse, Delinquenzprophylaxe, 135

³²⁶ Tiedemann – Sasse, Delinquenzprophylaxe, 7

³²⁷ Zur datenschutzrechtlichen Problematik von Werturteilen, Rill, Datenschutz in der Wirtschaft, 15 (19) sowie Duschanek, 51 (53) und Duschanek-Hierzenberger, 175 (182)

DSG 2000 nicht erfüllt und eine weitere Abwägung in Bezug auf schutzwürdige Interessen nicht gegeben.

Hiemit wird aufgezeigt, dass die Tätigkeit von Kreditauskunfteien, das Grundrecht auf Geheimhaltung personenbezogener Daten nicht beeinträchtigt.³²⁸ Aus diesem Grund sind auch die bei der Ermittlung angewandten Beschaffungsmethoden auf einen Widerspruch mit allfälligen schutzwürdigen Interessen nicht zu beachten, da diese überhaupt nicht vorhanden sind.³²⁹

Auskunfteien sind zur Beschaffung von Informationen für ihre Tätigkeit darauf angewiesen, dass sie Informationen von Banken, Lieferanten und sonstigen Geschäftspartnern des betroffenen Unternehmens/Person erheben und verarbeiten. Dadurch sind sie natürlich mit den Übermittlungsbeschränkungen des DSG sowie des BWG konfrontiert. Naturgemäß werden auch oft Selbstauskünfte von den befragten Firmen eingeholt und verarbeitet. Die Überprüfungsmöglichkeiten sind bei diesen Angaben naturgemäß eingeschränkt. Decken sich die eigenen Aufschlüsse mit Informationen von dritter Seite nicht, so wird dies in der Auskunft hervorgehoben. Branchenquerschnitte und Vergleiche mit entsprechenden Daten aus früherer Zeit ermöglichen eine Grobkontrolle wobei bestätigte Jahresabschlüsse eine sehr große Aussagekraft und Verlässlichkeit aufweisen.³³⁰

Prinzipiell werden in den erteilten Auskünften größtenteils nur Informationen erteilt, an denen das/die betroffene Unternehmen/Person kein schutzwürdiges Interesse beanspruchen können/kann. Die Erteilung von Informationen AN Auskunfteien erscheint unter der Betrachtung des § 8 Abs 1 Z 4 DSG 2000 im Hinblick auf das ihnen von der Rechtsordnung eingeräumten Rechts aufgrund der Gewerbeberechtigung des § 153 GewO als „überwiegendes berechtigtes Interesse“ als gerechtfertigt. Die in § 8 Abs 1 Z 4 DSG 2000 geforderte Interessensabwägung bereitet aufgrund der im Geschäftsleben notwendigen Transparenz über ein Unternehmen bzw. bestimmte Angaben über eine Person keine Schwierigkeiten.³³¹ Für den Fall der Auskunftserteilung kann wiederum § 8 Abs 1 Z 4 DSG 2000 herangezogen werden weil im vorliegenden Zusammenhang vom „berechtigten Interesse eines Dritten“ (=Auskunftsempfänger) gesprochen werden kann. Eine zugunsten des

³²⁸ So auch *Tiedemann-Sasse*, Delinquenzprophylaxe 130ff, 142; *Mallmann*, Kreditinformationsdienst und Datenschutz, Betriebsberater 1980, 1020 (1022); *Duschanek-Hierzenberger*, Datenschutz in der Wirtschaft, 175 (184)

³²⁹ *Stadler*, ÖZW 1979, 12; *Duschanek-Hierzenberger*, Datenschutz in der Wirtschaft, 175 (186)

³³⁰ *Tiedemann – Sasse*, Delinquenzprophylaxe, 43

³³¹ so auch *Stadler*, ÖZW 1979, 15

Betroffenen ausgehende Interessensabwägung wird nur in sehr spezifischen Fällen meistens welche die Achtung des Privat -und Familienleben betreffen, zu Tage treten.³³²

In Bezug auf Bankauskünfte über die wirtschaftliche Lage eines Unternehmers stellt § 38 Abs 2 Z 6 BWG insoweit eine Ausnahme vom Bankgeheimnis dar.

Wenn gleich auch der wirtschaftliche Schwerpunkt und die Aussagekraft von Auskünften auf dem Gebiet der Wirtschaftsauskünfte über Wirtschaftstreibende liegt, so ist aus den gewerberechtlichen Bestimmungen der §§ 29 und 153 GewO eine Beschränkung auf diesen Betroffenenkreis nicht zu entnehmen.

§ 153 GewO schließt zwar die Erteilung von Auskünften über private Verhältnisse aus wenn diese nicht im Zusammenhang mit der Kreditwürdigkeit stehen aber nicht die Auskunft über die Kreditwürdigkeit von Privatpersonen an sich. Die Gewerbeberechtigung erlaubt somit auch Kreditauskünfte über Personen, die nicht als Wirtschaftstreibende anzusehen sind, insbesondere Konsumenten. Dazu mehr in den nächsten Kapiteln.

³³² *Duschanek*, Datenschutz, 313; *Duschanek-Hierzenberger*, Datenschutz in der Wirtschaft, 175 (189)

10.2. KSV Wirtschaftsdatenbank

Die Einholung von Wirtschaftsauskünften ist heute aus dem modernen Geschäftsleben nicht mehr wegzudenken. Sie geben Ausschluss über die wirtschaftliche Lage und Bonität eines Unternehmens und vermindern dadurch das Verlustrisiko des Kreditgebers (Lieferanten) und sind in weiterer Folge auch von großer Bedeutung für die Volkswirtschaft. Die Einrichtung des Auskunftsgewerbes in der GewO stellt eine Maßnahme dar, die zum „wirtschaftlichen Wohl des Landes notwendig ist“ und womit einer der in § 8 Abs 2 MRK genannten Gründe vorliegt, wie er in § 1 Abs 2 DSG 2000 als mögliche Beschränkung des Grundrechtsanspruches vorgesehen ist.³³³

Der KSV betreibt seit seinem Bestehen im Jahre 1870 eine Wirtschaftsdatenbank in welcher protokollierte Unternehmen und sonstige Selbstständige enthalten sind. Diese wurde (erst) 1984 EDV unterstützt.

Die Datenbank hat folgenden Umfang: (*)

Jährlich getätigte Abfragen	500.000 - 600.000
Jährliche Rechercheaufträge	zigtausende (von 100 Mitarbeitern)
Firmenauskünfte	> 300.000(**)

(*) genauere Daten wurden leider nicht zur Verfügung gestellt

(**) durch Neugründungen und Löschungen mehrere 100.000 Firmendatenstämme

Der KSV bietet verschiedene Auskünfte mit verschiedenen Inhalten an. Kurz zusammengefasst kann gesagt werden, je mehr Informationen in der Auskunft enthalten sind desto umfangreicher und teurer wird sie.

³³³ So Hierzenberger in Duschaneck (Hrsg), Geheimnischutz im Wirtschaftsleben, 183

Professional	Standard	Compact	BonitätsReport	BilanzReport	BeteiligungsReport	FirmenbuchReport	FunktionsstrategieProfil	UID-Report	InsolvenzReport		
•	•	•	•	•	•	•	•	•	•	KSV-Nummer	KSV-Identifikationsnummer für Unternehmen und Personen
•	•	•	•	•	•	•	•	•	•	Adressblock	Exakte Firmenidentifikation mit Firmennamen, Sitz, Telefon, Fax, E-Mail und Internet
•	•	•	•	•	•	•	•	•	•	Status	Aktuelle Situation des Unternehmens, z. B. aktive Firma, in Gründung, ruhende Firma etc.
•	•	•	•	•	•	•	•	•	•	Branche	Branchenzugehörigkeit nach ÖNACE-Code
•	•	•	•	•	•	•	•	•	•	KSV-Rating	KSV-Rating zur Bewertung des Geschäftsrisikos; Vergleich zum durchschnittlichen KSV-Rating aller Unternehmen in der jeweiligen Branche
•	•	•	•	•	•	•	•	•	•	KSV-Empfehlung	Empfehlung der KSV-Experten für Engagements mit dem Unternehmen
•	•	•	•	•	•	•	•	•	•	Zahlweise	Zahlungsverhalten eines Unternehmens; beste Einstufung mit 100, schlechteste mit 600
•	•	•	•	•	•	•	•	•	•	Beurteilung	Aktuelle finanzielle Gesamtsituation des Unternehmens; beste Einstufung mit 100, schlechteste mit 600
•	•	•	•	•	•	•	•	•	•	Einzelhöchstkredit	Maximale Kreditempfehlung des KSV pro Lieferanten bei durchschnittlichem Zahlungsziel (60 Tage)
•	•	•	•	•	•	•	•	•	•	Insolvenzdaten	Tagaktuelle Insolvenzinformationen
•	•	•	•	•	•	•	•	•	•	Inkassofälle	KSV-Inkassofälle sowie aktueller Stand der Betreuung
•	•	•	•	•	•	•	•	•	•	Kennwerte	Kennwerte wie Umsatz, Warenlager, Forderungen, Verbindlichkeiten, Mitarbeiter etc.
•	•	•	•	•	•	•	•	•	•	Tätigkeit	Beschreibung der Geschäftstätigkeit
•	•	•	•	•	•	•	•	•	•	Registernummer	UID-Nummer, DVR-Nummer, ARA-Lizenz
•	•	•	•	•	•	•	•	•	•	Außenhandel	Import- und Exportquote mit Angabe der Länder
•	•	•	•	•	•	•	•	•	•	Firmenbuch	Tagaktuelle Daten aus dem österreichischen Firmenbuch über Rechtsform, Kapital, Gesellschafter, Vertretungsbefugnisse etc.
•	•	•	•	•	•	•	•	•	•	Management	Handelsrechtliche Funktionen der betreffenden Personen im angefragten Unternehmen sowie Anzahl weiterer handelsrechtlicher Funktionen in anderen Unternehmen
•	•	•	•	•	•	•	•	•	•	Grundbuch	Auszug aus dem Grundbuch mit Erklärungen
•	•	•	•	•	•	•	•	•	•	Bilanz	Werte aus der veröffentlichten Bilanz und GuV, inkl. Bilanzkennzahlen wie Eigenkapitalquote, Cashflow, Gesamtkapitalrentabilität, Schuldentilgungsdauer etc.
•	•	•	•	•	•	•	•	•	•	Branchenvergleich	Zusammenfassung der wesentlichen Informationen aus Bilanz und GuV sowie der Vergleich mit den Branchendurchschnittswerten
•	•	•	•	•	•	•	•	•	•	Standorte	Offizielle, operative und ehemalige Standorte
•	•	•	•	•	•	•	•	•	•	Beteiligungen	Beteiligungen an anderen Unternehmen und beteiligte Gesellschafter
•	•	•	•	•	•	•	•	•	•	Bankverbindung	Haupt- und Nebenbankverbindungen
•	•	•	•	•	•	•	•	•	•	Firmenhistorie	Wesentliche Ereignisse in der Geschichte des Unternehmens wie Gründungsjahr, Änderung des Firmenwortlauts, Verschmelzungen etc.
•	•	•	•	•	•	•	•	•	•	Grafiken	Grafische Darstellung der Entwicklung von KSV-Rating, Inkassofällen, Umsatz und Umsatz pro Mitarbeiter

Anhand des unten angeführten Musterbeispiels „Professional“ lässt sich erkennen wie genau und detailliert und mit welcher Tiefe allgemeine als auch Bonitätsinformationen über Unternehmen zur Verfügung gestellt werden können:

KSV1870

KSV-Auskunft UnternehmensProfil Professional

Zuletzt überarbeitet am: 2008-06-06
Datum und Uhrzeit der Abfrage: 2008-07-01 12:55
Auskunft bestellt am: 2008-07-01 12:55
Auftragsnummer: 100012130728
Auftraggebernummer: 1265019
Auftraggeber: KSVMM007
Referenz: KSVMM007

KSV-Inkasso-, Insolvenz- und Firmenbuchdaten sind tagaktuell.
Zuletzt überarbeitet am gibt den Zeitpunkt der letzten kompletten Überprüfung durch den KSV an.

Ihre Anfrage:
Max Meier Test GmbH & Co. KG. (TESTFIRMA) , Wagenseilgasse 7, A-1120 Wien

Firmenbasisinformation:

KSV-Nummer: ☐ 49054
Zuletzt überarbeitet am: ☐ 2008-06-06
Name: Max Meier Test GmbH & Co. KG. (TESTFIRMA)
Status: ☐ aktive Firma
Adresse: Wagenseilgasse 7, A-1120 Wien
Telefon: 0043 (1) 123456
Fax: 0043 (1) 123456 - 789
E-Mail: meier@testfirma.at
Internet: <http://www.testfirma.at>
Branche: ☐ Önace 514201 85% Großhandel mit Bekleidung
Önace 182201 15% Herstellung von sonstiger Damen- und Mädchenoberbekleidung
Gesamtbewertung: **Rating** ☐ 413 (PD 2,34% ☐ nach Basel II)
Erhöhtes Risiko
Das KSV-Rating des Unternehmens ist schlechter als der Branchendurchschnitt.
Empfehlung
Aufgrund unterschiedlicher Erfahrungen aus dem Branchen- und Unternehmensumfeld empfiehlt der KSV, bei Geschäfts- und Kreditverbindungen Sicherheiten einzufordern.
Detailbewertungen: **Zahlweise** ☐ 400
Das Unternehmen zahlt heute in der Nettofrist oder nach mehrmaliger Mahnung. Es bestehen auch Sondervereinbarungen. In der Vergangenheit kam es auch zu gerichtlichen Betreibungen.
Beurteilung ☐ 400
Das Unternehmen ist ausschließlich auf Fremdkapital angewiesen, fallweise treten Liquiditätsengpässe auf. Die Ertragslage war zuletzt nicht zufriedenstellend.
KSV-Einzelhöchstkredit ☐ EUR 5.000,00

Negativinformationen von Dritten:

Datum	Betrag	Status
2006-12-24		Grav. Zahlungsanstände liegen vor

Firmenzusatzinformationen:

Gründungsjahr: 1974
Rechtsform: Kommanditgesellschaft seit 1974-10-01
Firmenbuchnummer: ☐ FN 900000 a Wien seit 1974-11-20
Tätigkeitsbereich: Betrieben wird der Großhandel mit klassischer Damen- und Herrenoberbekleidung, wobei vorwiegend auf eigene Rechnung gearbeitet wird. In kleinerem Rahmen führt man auch eine eigene Produktion von Damenblusen, welche unter der Markenbezeichnung "Gloria" in den Handel kommen.
Firmen Typ: Großhandel
Aliasname: ☐ GLORIA
UID: ☐ ATU 23456789

Import	Land	Bezugsjahr
Import	Tschechische Republik	2007
Import	Slowakische Republik	2007

Export	Land	Bezugsjahr
Export	Frankreich	2007
Export	Deutschland	2007

Kennwerte: ☐

Umsatz gesamt	2007	EUR 670.000,00 (erwartet)
Umsatz gesamt	2006	EUR 643.855,88 (genau)
Umsatz gesamt	2005	EUR 538.596,34 (genau)
Umsatz gesamt	2004	EUR 519.820,67 (genau)
Umsatz gesamt	2003	EUR 500.115,00 (genau)
Beschäftigte gesamt	2007	4 (genau)
Beschäftigte gesamt	2006	6 (genau)
Beschäftigte gesamt	2005	7 (genau)
davon Angestellte	2007	3 (genau)
davon Angestellte	2006	4 (genau)
davon Arbeiter	2007	1 (genau)
davon Arbeiter	2006	2 (genau)
Warenlager gesamt	2007	EUR 250.000,00 (durchschnittlich)
Forderungen gesamt	2007	EUR 450.000,00 (circa Kunden)
Verbindlichkeiten gesamt	2007	EUR 150.000,00 (circa Lieferanten)
Fuhrpark gesamt	2007	2 (genau)
davon PKW	2007	1 (genau)
davon LKW bis 3,5t	2007	1 (genau)

Grundbuch: ☐

Einlagezahl 1484 Katastralgemeinde 01004 Innere Stadt WPG: Wien Tagebuchkennzahl 11/2007 Stand-Per 2007-07-08

Teil A - Art der Liegenschaft :

Plombe 607/2007
 GST-NR G BA (NUTZUNG) FLÄCHE GST-ADRESSE
 Baufl.(Gebäude) 859 Zelinkagasse 10
 Gonzagagasse 20
 1 a 843/2001 Bauplatz (auf) Gst .9
 2 a 843/2001 Verpflichtung zur Herstellung der Höhenlage und zur Übergabe gem Pkt 1 Bescheid 1936-12-01

Teil B - Eigentumsverhältnisse :

1 ANTEIL: 1/1
 Max Meier Test GmbH & Co. KG.
 ADR: Wagenseilgasse 7, 1120 Wien
 a 2758/2003 Urkunde 2003-07-14 Eigentumsrecht
 d 11/2007 Rangordnung für die Veräußerung bis 2007-07-07

Teil C - Belastungen :

3 b 3996/2003 IM RANG 11/2003 Pfandurkunde 2003-05-21
 PFANDRECHT Höchstbetrag
 EUR 610.000,--
 für Bank Austria Creditanstalt AG

Personendaten:

Person ☐	Geburtsdatum	Adresse	Funktion ☐	Weitere handelsrechtliche Funktionen ☐
<u>Dipl.-Ing.Dr. Max Erich Meier</u>	1965-12-24	1120 Wien Wagenseilgasse 7	Einzelprokurist, Leiter Verkauf, Leiter Marketing	2
Er ist Vater von drei Kindern. Dipl.-Ing. Dr. Max Erich Huber war ehemals unselbständig im Rahmen eines Schweizer Pharmakonzerns beschäftigt. Eine aufrechte Gewerbeberechtigung liegt für ihn derzeit nicht auf (letzte Überprüfung 10.10.2007).				
<u>Eva Meier</u>	1936-06-06	1120 Wien Wagenseilgasse 7	Kommanditist, Leiter Rechnungswesen, Leiter Einkauf, Leiter EDV	2
Sie ist Mutter von 2 Söhnen.				

Bilanz (absolute) ☐ alle Beträge in EUR

2006-12-31 Abw. 2005-12-31 Abw. % 2004-12-31

Fertige Erzeugnisse		29,76	16,36
Noch nicht abrechenbare Leistungen		0,67	6,08
Vorräte	27,15		
Summe Vorräte	27,15	30,46	22,45
Forderungen aus Lieferungen und Leistungen		10,38	41,92
Sonstige Forderungen und Vermögensgegenstände		11,98	0,39
Forderungen und sonstige Vermögensgegenstände	43,42		
Summe Forderungen	43,42	22,35	42,32
Kassenbestand, Schecks, Guthaben bei Banken	0,06	0,03	0,24
Summe Kassa und Bank	0,06	0,03	0,24
Summe Umlaufvermögen	70,62	52,84	65,00
Aktive Rechnungsabgrenzung	6,36	5,72	2,25
Summe ARA	6,36	5,72	2,25
Aktiva	100,00	100,00	100,00
Gezeichnetes, bzw. gewidmetes Kapital	6,81	10,15	6,37
Gebundene Kapitalrücklagen	54,98	81,93	51,44
Bilanzgewinn (Bilanzverlust)	-234,27	-269,91	-117,44
Atypisch Stille Einlagen	-5,25	-7,83	
Summe Eigenkapital	-177,73	-185,66	-59,62
Rückstellungen für Abfertigungen		2,54	1,83
Sonstige Rückstellungen		3,11	11,71
Rückstellungen	5,74		
Summe Rückstellungen	5,74	5,66	13,53
Verbindlichkeiten gegenüber Kreditinstituten		147,08	68,31
Stille Gesellschaft		57,95	36,38
Verbindlichkeiten aus Lieferungen und Leistungen Verbindlichkeit aus der Annahme gezogener und der Ausstellung eigener Wechsel		19,07	6,28
Sonstige Verbindlichkeiten		55,90	35,12
Verbindlichkeiten	271,98		
Summe Verbindlichkeiten	271,98	280,00	146,09
Passiva	100,00	100,00	100,00
Eventualverbindlichkeiten	5,25	7,83	
Bilanzsumme	100,00	100,00	100,00

GuV (absolute) alle Beträge in EUR

	2006-12-31	Abw. %	2005-12-31	Abw. %	2004-12-31
Bruttoumsatzerlöse			538.596,34	-68,68	1.719.820,67
Roherträge	643.855,88				
Erhöhung oder Verminderung des Bestands an fertigen und unfertigen Erzeugnissen sowie an noch nicht abrechenbaren Leistungen			-62.166,00	-542,05	14.063,00
Umsatzerlöse gesamt oder Roherträge Gesamt	643.855,88	35,14	476.430,34	-72,52	1.733.883,67
Erträge aus Auflösung von Rückstellungen			109.970,70		
Übrige betriebliche Erträge	149.845,84	27,65	117.386,05	-50,31	236.241,45
Sonstige betriebliche Erträge gesamt	149.845,84	-34,09	227.356,75	-3,76	236.241,45
Aufwendungen für bezogene Leistungen			-181,50	96,49	-5.169,44
Spezialkonto Materialaufwand			-257.367,50	28,44	-359.657,25
Materialaufwand gesamt			-257.549,00	29,41	-364.826,69
Löhne	-55.706,93	-85,71	-29.996,54	46,39	-55.956,15
Gehälter	-352.001,85	-11,30	-316.251,79	-12,65	-280.730,84
Aufwendungen für Abfertigungen	-15.452,47	-705,98	2.550,00	166,99	-3.806,51
Gesetzliche Sozialabgaben sowie sonstige vom Entgelt abhängige Abgaben	-117.438,44	-19,62	-98.174,77	-5,58	-92.983,03
Sonstige Sozialaufwendungen	-9.485,19	-49,12	-6.360,74	-147,73	-2.567,58
Personalaufwand gesamt	-550.084,88	-22,72	-448.233,84	-2,80	-436.044,11
Abschreibungen auf immaterielle Vermögensgegenstände, Sachanlagen, aktivierte Aufwendungen für das Ingangsetzen und Erweitern eines Betriebes	-146.467,69	32,38	-216.603,45	6,04	-230.526,20
Abschreibungen/Sachanlagen/imm.AV gesamt	-146.467,69	32,38	-216.603,45	6,04	-230.526,20
Verschiedene betriebliche Aufwendungen	-565.265,28	-51,89	-372.143,93	22,31	-479.024,80
Sonstige Steuern	-12.782,51	-682,36	-1.633,85	65,83	-4.782,22
Summe Betriebsaufwand Steuern	-578.047,79	-54,65	-373.777,78	22,74	-483.807,02

Betriebsergebnis gesamt	-480.898,64	18,82	-592.376,98	-230,22	454.921,10
Zinserträge, Wertpapiererträge und ähnliche Erträge	76,57	61,78	47,33	-79,91	235,62
Erlöse aus dem Abgang von sonstigen Finanzanlagen	558,07				21,52
Zinsen und ähnliche Aufwendungen	-62.276,90	35,09	-95.950,02	-36,09	-70.505,25
Finanzergebnis gesamt	-61.642,28	35,72	-95.902,69	-36,52	-70.248,11
EGT gesamt	-542.540,90	21,17	-688.279,67	-278,93	384.672,99
Steuern vom Einkommen und vom Ertrag	-3.500,00	-223,10	2.843,15	101,69	-168.498,84
Steuern gesamt	-3.500,00	-223,10	2.843,15	101,69	-168.498,84
Jahresüberschuß/Fehlbetrag gesamt	-546.040,90	20,34	-685.436,52	-417,08	216.174,15
Jahresgewinn/Jahresverlust gesamt	-546.040,90	20,34	-685.436,52	-417,08	216.174,15
Gewinnvortrag/Verlustvortrag aus dem Vorjahr (Gewinn/Verlustrechnung)	-1.861.323,82	-44,30	-1.289.887,30	14,35	-1.506.061,45
Gewinnabfuhr bzw. Verlustüberrechnung aus Ergebnisabführungsverträgen			114.000,00		
Vorträge gesamt	-1.861.323,82	-58,29	-1.175.887,30	21,92	-1.506.061,45
Bilanzgewinn/Bilanzverlust aus Gewinn/Verlustrechnung	-2.407.364,72	-29,34	-1.861.323,82	-44,30	-1.289.887,30

GuV (relative) [1]

	2006-12-31	2005-12-31	2004-12-31
Bruttoumsatzerlöse		113,05	99,19
Roherträge	100,00		
Erhöhung oder Verminderung des Bestands an fertigen und unfertigen Erzeugnissen sowie an noch nicht abrechenbaren Leistungen		-13,05	0,81
Umsatzerlöse gesamt oder Roherträge Gesamt	100,00	100,00	100,00
Erträge aus Auflösung von Rückstellungen		23,08	
übrige betriebliche Erträge	23,27	24,64	13,62
Sonstige betriebliche Erträge gesamt	23,27	47,72	13,62
Aufwendungen für bezogene Leistungen		-0,04	-0,30
Spezialkonto Materialaufwand		-54,02	-20,74
Materialaufwand gesamt		-54,06	-21,04
Löhne	-8,65	-6,30	-3,23
Gehälter	-54,67	-66,38	-18,19
Aufwendungen für Abfertigungen	-2,40	0,54	-0,22
Gesetzliche Sozialabgaben sowie sonstige vom Entgelt abhängige Abgaben	-18,24	-20,61	-5,36
Sonstige Sozialaufwendungen	-1,47	-1,34	-0,15
Personalaufwand gesamt	-85,44	-94,08	-25,15
Abschreibungen auf immaterielle Vermögensgegenstände, Sachanlagen, aktivierte Aufwendungen für das Ingangsetzen und Erweitern eines Betriebes	-22,75	-45,46	-13,30
Abschreibungen/Sachanlagen/Imm.AV gesamt	-22,75	-45,46	-13,30
Verschiedene betriebliche Aufwendungen	-87,79	-78,11	-27,63
Sonstige Steuern	-1,99	-0,34	-0,28
Summe Betriebsaufwand Steuern	-89,78	-78,45	-27,90
Betriebsergebnis gesamt	-74,69	-124,34	26,24
Zinserträge, Wertpapiererträge und ähnliche Erträge	0,01	0,01	0,01
Erlöse aus dem Abgang von sonstigen Finanzanlagen	0,09		0,00
Zinsen und ähnliche Aufwendungen	-9,67	-20,14	-4,07
Finanzergebnis gesamt	-9,57	-20,13	-4,05
EGT gesamt	-84,26	-144,47	22,19
Steuern vom Einkommen und vom Ertrag	-0,54	0,60	-9,72
Steuern gesamt	-0,54	0,60	-9,72
Jahresüberschuß/Fehlbetrag gesamt	-84,81	-143,87	12,47

Jahresgewinn/Jahresverlust gesamt	-84,81	-143,87	12,47
Gewinnvortrag/Verlustvortrag aus dem Vorjahr (Gewinn/Verlustrechnung)	-289,09	-270,74	-86,86
Gewinnabfuhr bzw. Verlustüberrechnung aus Ergebnisabführungsverträgen		23,93	
Vorträge gesamt	-289,09	-246,81	-86,86
Bilanzgewinn/Bilanzverlust aus Gewinn/Verlust-rechnung	-373,90	-390,68	-74,39

Bilanzkennzahlen ^[1]

	2006	Abw. %	2005	Abw. %	2004	Branchen- durchschnitt
Cash Flow II ^[1]	-399.573,21	+14,77	-468.833,07	-204,95	446.700,35	
Schuldentilgungsdauer ^[1]	-7,14	-70,00	-4,20	-207,42	3,91	8,88
Bankverschuldung ^[1]	0,00	-100,00	147,08	+115,34	68,30	
Eigenkapitalquote ^[1]	-177,72	+4,27	-185,65	-211,39	-59,62	14,06
Sozialkapitalquote ^[1]	0,00	-100,00	2,54	+39,56	1,82	
Anlagendeckung I ^[1]	-772,08	-74,73	-441,87	-150,39	-176,47	180,10
Umsatzrentabilität ^[1]	0,00	+100,00	-144,46	-751,31	22,18	
Kapitalumschlag ^[1]	0,00	-100,00	0,69	-56,05	1,57	
Gesamtkapitalrentabilität (ROI) ^[1]	-46,73	+45,59	-85,89	-307,26	41,44	7,98
Cash Flow in % der Betriebsleistung ^[1]	0,00	+100,00	-98,40	-481,99	25,76	
Cash Flow I ^[1]	-396.073,21	+16,03	-471.676,22	-176,67	615.199,19	
Bruttoproduktivität ^[1]	0,00	-100,00	1,06	-73,30	3,97	
Nettoproduktivität ^[1]	0,00	-100,00	0,48	-84,66	3,13	
Betriebsleistung ^[1]	0,00	-100,00	476.430,34	-72,52	1.733.883,67	
Vorräte in Prozent der Betriebsleistung ^[1]	0,00	-100,00	44,08	+210,20	14,21	
Rohertrag ^[1]	0,00	-100,00	218.881,34	-84,01	1.369.056,98	

^[1] *Die Branchendurchschnittswerte der Kennzahlen werden von der KMU FORSCHUNG AUSTRIA (Austrian Institute for SME Research) auf Basis anonymisierter Bilanzdaten österreichischer Unternehmen zur Verfügung gestellt.

Branchenvergleich ^[1]

Eigenkapitalquote	Die Eigenkapitalquote des Unternehmens ist schlechter als der Branchendurchschnitt.
Cash Flow in % der Betriebsleistung	kein Branchenvergleich vorhanden
Gesamtkapitalrentabilität (ROI)	Die GK-Rentabilität des Unternehmens ist schlechter als der Branchendurchschnitt.
Schuldentilgungsdauer	Die errechnete Schuldentilgungsdauer ist negativ.

Standorte

Art	Straße	Telefon	Fax	Beschreibung
				e-Mail
offiziell	A-1120 Wien, Wagenseilgasse 7			protokollierter Sitz, Mieträumlichkeiten
operativ	A-1120 Wien, Wagenseilgasse 7			Firmensitz, Mieträumlichkeiten
		0043 1 123456	0043 1 123456	meier@testfirma.at
		789		
operativ	A-4020 Linz, Mozartstraße 11			Niederlassung, Pachträumlichkeiten
operativ	A-1010 Wien, Zelinkagasse 10			Büro, Eigentumsobjekt
operativ	A-8010 Graz, Wielandgasse 14			Lager, Leasingobjekt
ehemalig	A-1090 Wien, Müllnergasse 8			Firmensitz

Beteiligungen und nahestehende Unternehmen:

Name

PLZ

KSV Nummer Firmenbuch

An diesem Unternehmen ist beteiligt:

Testfirma Max Meier Gesellschaft m.b.H. Wagenseilgasse 7, A-1120 Wien %

101.959 FN 900001 b

Bankverbindungen:

Bank

BLZ

Verbindungsart

Erste Bank der oesterreichischen Sparkassen AG, 1011 Wien
Kontokorrentkredit

20111

Hauptverbindung
EUR 100.000,00

Raiffeisen Zentralbank Österreich Aktienges., 1011 Wien

31000

debitorische Verbindung

Bank Austria Creditanstalt AG, 1011 Wien

20151

Hypothekerverbindung

Historische Entwicklung:

Gründungsjaar:

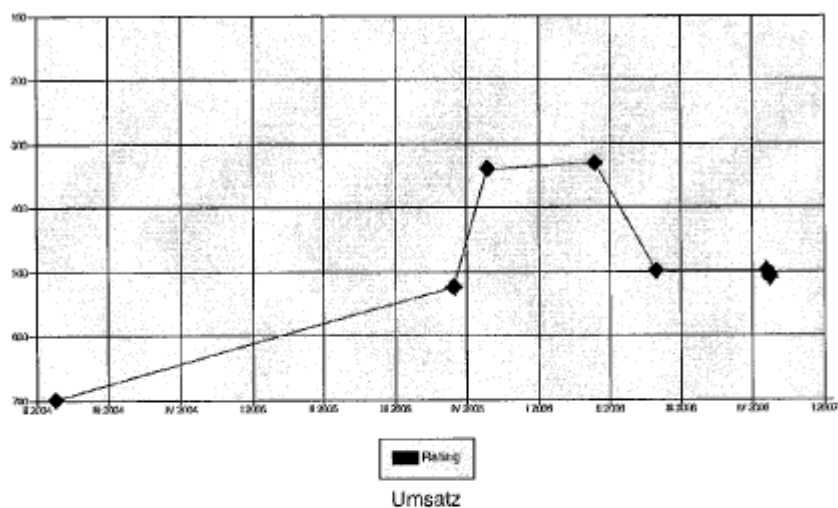
1974

Protokollierungsdatum:

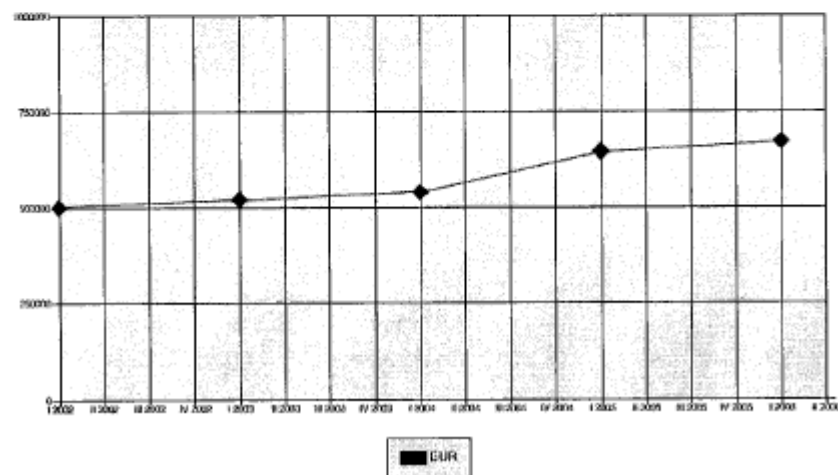
1974-11-20

Grafiken:

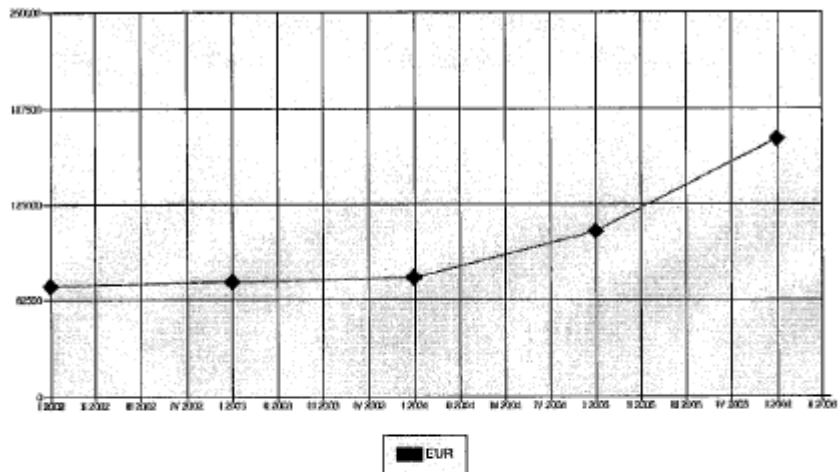
Rating



Umsatz



Umsatz pro Mitarbeiter



KSV1870 Information GmbH
Wagenseilgasse 7
A-1120 Wien

Bei Fragen erreichen Sie unser Customer Care Center unter der österreichweiten Telefonnummer:
050 1870-1000
e-mail: ksv@ksv.at

Diese Informationen sind nur für Ihren internen Firmengebrauch bestimmt und unterliegen sowohl den Allgemeinen Geschäftsbedingungen der KSV1870 Information GmbH als auch den Bestimmungen Ihres Vertrages.

Nach den Bestimmungen des Datenschutzgesetzes dürfen die übermittelten Informationen nur für den Zweck verarbeitet oder genutzt werden, für dessen Erfüllung sie angefordert wurden. Die Verarbeitung oder Nutzung für andere Zwecke oder für Zwecke Dritter ist ausgeschlossen.
FN 308571 g
Copyright © KSV1870 Information GmbH

Ende des Dokuments

[Zurück zur Übersicht](#)

10.2.1. Die wichtigsten Daten und Fakten in der KSV Wirtschaftsdatenbank

Unternehmensstammdaten	Art der Erhebung	Anzahl der Unternehmen
Eintragung/Änderungen im Firmenbuch Firmennamen Protokollierungsdaten Management und Eigentümer/Teilhaber	tägliche automatische Verarbeitung	ca. 170.000 Unternehmen, 100-prozentige Abdeckung der im Firmenbuch eingetragenen österreichischen Unternehmen. Historische Daten vorhanden seit 1. 1. 1997
Status (aktiv, ruhend, gelöscht) Firmenadressen Gründungsjahr Unternehmenstätigkeit Außenhandelsaktivitäten Branchenzuordnung Bankenverbindung Unternehmenskennwerte (Umsatz, Beschäftigte, Warenlager, Fuhrpark) Firmenhistorie	von KSV-Experten erhoben	ca. 300.000 Unternehmen, mehr als 160.000 Aktualisierungen pro Jahr. Historische Daten vorhanden seit 1. 1. 1997
Grundbuch (soweit Liegenschaft vorhanden)	regelmäßige Aktualisierungen	ca. 90.000 Unternehmen
Gewerbeberechtigungen	von KSV-Experten erhoben und bewertet	ca. 160.000 Unternehmen
Personenfunktionsträger	tägliche automatische Verarbeitung aus dem Firmenbuch, Bereichsfunktionsträger (z. B. Leiter Rechnungswesen) werden von KSV-Experten erhoben	ca. 960.000 Personen
Firmenverknüpfungen, Konzernverbindungen wie z. B. Beteiligungen	tägliche automatische Verarbeitung aus dem Firmenbuch	

Bonitätsdaten	Art der Erhebung	Anzahl der Unternehmen
Bankauskünfte (§ 38 BWG9)	von KSV-Experten erhoben und bewertet	
Bilanzen, Geschäftsberichte	automatische Einholung bei Firmenbuchgerichten, erhoben, von Unternehmen zur Verfügung gestellt	Verarbeitung aktueller Bilanzen zu über 70.000 Unternehmen pro Jahr. Historische Daten vorhanden seit 1.1.1997
Zahlweiseinformationen	von KSV-Experten erhoben und bewertet	ca. 300.000 Unternehmen
Debitoreninformationen	von Mitgliedern des KSV zur Verfügung gestellt	Verarbeitung von ca. 200.000 Fakturenpositionen pro Monat
Gerichtliche und außergerichtliche Inkassoinformationen	von KSV-Experten erhoben und bewertet	Daten zu über 100.000 Unternehmen. Historische Daten vorhanden
Insolvenzinformationen	Art der Erhebung	
Gerichtliche und außergerichtliche Insolvenzinformationen	von den Konkursgerichten, von den Schuldern und Gläubigern bzw. deren Vertretern, Ediktsdatei, des BM für Justiz	gerichtliche Insolvenzen und abgewiesene Konkursanträge zu 100% seit 1. 1. 1992, Konkursanträge von dritter Seite, soweit bekannt; außergerichtliche Insolvenzen, soweit bekannt, seit 1. 1. 1992

10.2.2. Ratingkennzahlen und ihre Bedeutung

KSV-Rating	KSV-Neu-gründerScore	Risiko	Ausfallsrisiko	
100-199		keines	Risiko liegt unter dem Durchschnitt	Go
200-299	200, 250	sehr gering		
300-399	300, 350	gering		
400-499	400, 450	erhöht	Risiko liegt über dem Durchschnitt	Stop
500-599	500, 550	hoch		
600-699	600	sehr hoch		
700		Insolvenz		

Unter Berücksichtigung sämtlicher Einflussfaktoren ergeben sich die Kennzahlen des KSV-Ratings, wobei mit aufsteigender Zahl die zunehmende Negativeinstufung zum Ausdruck kommt.

Beim KSV-Rating reicht die Skala von 100 bis 700; dieser Scorewert wird bis auf die dritte Ziffer genau berechnet. Der KSV-Neugründer Score wird auf einer Skala von 200 bis 600 in 50er-Schritte dargestellt.

Unternehmen mit einem Scorewert von unter 400 haben ein unterdurchschnittliches Insolvenzrisiko. Bei Unternehmen mit einem Wert über 400 liegt das Ausfallsrisiko über dem österreichischen Durchschnitt. Ratings werden im KSV normalerweise „unsolicited“ durchgeführt, d. h., der KSV tritt an die zu ratenden Unternehmen heran, ohne von diesen dazu beauftragt worden zu sein. Zur Erstellung eines „solicited“ Ratings müssten Unternehmen eine Ratingagentur zu entsprechenden Konditionen beauftragen was wiederum mit relativ hohen Kosten verbunden wäre.

Zu den Adressaten eines Ratings (egal ob „unsolicited“ oder „solicited“) zählen vor allem Lieferanten weil mit ihnen häufig ein Kreditverhältnis in Form aus Lieferungen und Leistungen besteht bzw. bestehen wird, aber auch Kunden wenn sie zB durch Anzahlungen bereits in Vorleistung gegangen sind. Aufgrund der gestiegenen Unternehmensinsolvenzen in den letzten Jahren (siehe Kapitel II/S....) sind viele Lieferanten mit der unbesicherten

Lieferung von Waren und der damit verbundenen Kreditierung vorsichtiger geworden. Schließlich wirken sich hier größere Ausfälle direkt auf die wirtschaftliche Situation des jeweiligen Lieferanten aus. Ratings und Bonitätsbeurteilungen haben deshalb einen beträchtlichen Aussagewert, liefern sich doch aller Voraussicht nach eine Einschätzung des Delkrederisikos und der Zahlungssicherheit. Einen noch größeren Einfluss und Auswirkungen haben Ratings wenn eine sie zur Voraussetzung für die Aufnahme oder Fortsetzung einer Geschäftsverbindung werden. Großunternehmen wollen damit sicherstellen, dass ein Auftragnehmer hiemit seine wirtschaftliche Leistungsfähigkeit nachweist und damit jetzt und in nächster Zukunft in der Lage sein wird seine vereinbarte geschäftliche Leistung zu erbringen.³³⁴

10.2.2.1. KSV Neugründer Score

Zur Berechnung des KSV-Ratings sind viele „hard facts“ wie zB Bilanzen, Kennzahlen, langjährige Zahlungserfahrungen, etc. vorhanden.

Im Unterschied dazu habe die Faktoren im KSV-Neugründer Score eine starke statistische Ausprägung, da noch keine wesentlichen Erfahrungen vorliegen. Zusätzlich wird hier jedoch stark auf die Person des Jungunternehmers fokussiert. Neben den Faktoren aus der Struktur des Unternehmens und aus seinem Umfeld werden auch Parameter mit Bezug auf die Person des Neugründers berücksichtigt. (unter Einbeziehung historischer Erfahrungen)

Prinzipiell ist ein Ratingurteil einer externen Auskunft als Prognose einzustufen weil sie über die Wahrscheinlichkeit der vertragsgemäßen Erfüllung von Liefer- und Leistungsverpflichtungen handelt. Damit ist aber keine Garantie über den Eintritt eines bestimmten Erfolgs verbunden. Infolge des Prognosecharakters und der zukünftigen Unsicherheit sind diese nicht als Tatsachenbehauptung zu qualifizieren und es ob es zum Zeitpunkt der Festsetzung als richtig oder falsch zu qualifizieren ist, ist dem Beweis nicht zugänglich. Sie sind deshalb als ein subjektives Werturteil, eine Meinungsäußerung über wie wirtschaftliche Bonität eines Unternehmens zu sehen und sind in dieser Hinsicht einer gerichtlichen Überprüfung in Hinblick auf die inhaltliche Richtigkeit, entzogen.³³⁵

³³⁴ *Hundt/Neitz/Grabau*, Rating als Chance für kleinere und mittlere Unternehmen, 55ff; *Vetter*,...,1701

³³⁵ *Niedostadek*, Rating, 138; *Peters* (2001), 53

10.2.2.2. Berechnungsmodell des KSV-Ratings im Detail

(große Bilanzen)

Schuldentilgungsdauer I	Zeigt den kürzestmöglichen Zeitraum in Jahren an, in dem die Schulden aus eigener Kraft getilgt werden können. Dabei wird von der derzeitigen Ertragssituation sowie von der Annahme ausgegangen, dass der gesamte Cashflow zu eben dieser Tilgung (und nicht für Investitionen, Rücklagendotationen und Ausschüttungen) eingesetzt wird.	Je geringer, desto besser.
Liability Structure	Setzt den Anteil der kurzfristigen Verbindlichkeiten in Bezug zu den Gesamtverbindlichkeiten. Je langfristiger ein Unternehmen finanziert, desto besser die Stabilität und Liquidität. Liefer-, Bank- und Wechselverbindlichkeiten / Rückstellungen + Verbindlichkeiten	Je geringer, desto besser.
Eigenkapitalquote	Anteil des eigenen Kapitals am Gesamtkapital; ein Indikator für die Stabilität des Unternehmens. Die Erhöhung des Eigenkapitals bedingt auch eine Verbesserung der Bonität und Kreditwürdigkeit.	Je höher, desto besser.
Net Working Capital	Der Anstieg von Lieferantenverbindlichkeiten im Verhältnis zum Handelswarenvorrat signalisiert eine Streckung des Zahlungszieles und damit verbunden schlechte Liquidität des Unternehmens. Dadurch wird der Cashbestand im Zyklus erhöht; widmungsgemäß werden kurzfristige Verbindlichkeiten aufgebaut.	Je höher, desto besser.

Lagerintensität	In Relation zur Betriebsleistung sollten sich die Vorräte bei Expansion nicht nennenswert verändern. Kontinuierlich fallende Lagerintensitäten lassen auf eine Verlustverdeckung schließen, der tatsächlich erwirtschaftete Gewinn ist niedriger als der ausgewiesene; entweder werden stille Reserven bei den Vorräten aufgelöst, oder es erfolgt eine Überbewertung der Vorratsstände. Umgekehrt lässt eine Steigerung der Lagerintensitäten auf eine Gewinnverdeckung schließen.	Je geringer, desto besser.
Bilanzsumme		Je höher, desto besser.

10.2.2.3. Berechnungsmodell kleine Bilanzen

Eigenkapitalquote	Anteil des eigenen Kapitals am Gesamtkapital; ein Indikator für die Stabilität des Unternehmens. Die Erhöhung des Eigenkapitals bedingt auch eine Verbesserung der Bonität und Kreditwürdigkeit.	Je höher, desto besser.
Wachstum der Eigenkapitalquote	Eine Verbesserung des Eigenkapitals in Relation zur Bilanzsumme bedeutet Sicherung der Kapitalkraft durch Erhöhung des langfristigen Kapitals; ein Indikator für gute Ertragskraft oder Verbesserung der Außenfinanzierung.	Je höher, desto besser.
Lagerintensität	Ein überhöhter Lagerbestand wirkt sich aufgrund der Kapitalbindung ungünstig auf die Rentabilität aus. Eine Erhöhung der Lagerintensität kann schlechte Auftragslage oder Projektgeschäft bedeuten.	Je geringer, desto besser.

Liquidität	Die Kennzahl ist ein Indikator dafür, ob ein Betrieb bei Veräußerung des gesamten kurzfristigen Vermögens seinen kurzfristigen Zahlungsverpflichtungen nachkommen kann. Dem liegt die Annahme zugrunde, dass kurzfristig gebundenes Vermögen auch kurzfristig finanziert sein kann.	Je höher, desto besser.
Anlagedeckung	Nach der traditionellen „goldenen Bilanzregel“ muss dauernd im Betrieb verbleibendes Vermögen durch langfristige Kapitalpositionen abgesichert sein. Werte unter 100% bedeuten eine ungünstige Finanzierungssituation, die auch Liquiditätsschwierigkeiten nach sich ziehen kann.	Je höher, desto besser.
Bilanzgewinn	Bilanzgewinn – Gewinnvortrag.	Je höher, desto besser.
Bilanzsumme		Je höher, desto besser.
Berechnungsmodell: KSV-Beurteilung		
KSV-Beurteilung	Experteneinschätzung des KSV auf einer Skala von 100 bis 650.	Je geringer, desto besser.

10.2.2.4. Berechnungsmodell Strukturdaten (weiche Faktoren)

Zahlweise	Experteneinschätzung des KSV auf einer Skala von 100 bis 650.	Je geringer, desto besser.
Inkasso/Umsatz	Vorhandene KSV-Inkassofälle über 180,- EUR fließen in Relation zum Umsatz des Unternehmens ein.	Je geringer, desto besser.
Höhe der offenen Inkassofälle		Je geringer, desto besser.
Branchenzugehörigkeit	Gemäß ÖNACE-Code.	abhängig von Branchenzugehörigkeit
Rechtsform		abhängig von Rechtsform
Unternehmensalter		abhängig von Unternehmensalter
Umsatzwachstum		Je höher, desto besser.
Negativerfahrungen		Je weniger, desto besser.
Anzahl der Personen mit eingetragenen Funktionen	Bewertung der Entscheidungsstruktur im Unternehmen.	je mehr, desto besser. 336

³³⁶ Alle Fakten und Zahlen aus „KSV-Risikobewertung Details und Hintergründe“

10.2.3. Rechtliche Beurteilung

Die Umsetzung der „Richtlinie 96/9 EG des Europäischen Parlaments und des Rates vom 1. März 1996 über den rechtlichen Schutz von Datenbanken“ in das österreichische Recht wurde mit der UrhGNov 1997 (BGBl I 1998/25 vom 9. Jänner 1998) veranlasst. Da vielen (u.v.a. den „großen“) Datenbanken der große finanzielle, zeitliche und organisatorische Aufwand immanent ist, stellen sich diesbezüglich natürlich urheberrechtliche Fragen nach Installation einer solchen. Bis zu diesem Zeitpunkt kam solchen Datenbanken nur der Urheberrechtsschutz zu wenn es sich um eine „originelle“ (im Sinne von Originalität) Datenbank als Werk der Literatur, Tonkunst, der bildenden Künste oder Lichtbildkunst handelte. Ebenso zählt der OGH³³⁷ „Sammelwerke“ wie Enzyklopädien, Anthologien, Koch- und Adressbücher, Ausstellungskataloge, Zeitungen und Zeitschriften hiezu. Da große Datenbanken idR nach Vollständigkeit und nicht nach Originalität streben, bestand bis zu diesem Zeitpunkt ein Rechtsschutzdefizit da nach den Regeln des UrhRG eine vollständige Übernahme nicht unterbunden werden konnte. Erst durch Kapitel III der Richtlinie wurde ein „*Schutzrecht sui generis*“ geschaffen.³³⁸ Geschützt ist darin auch eine durch juristische Person erstellte Datenbank wenn für die Beschaffung, die Überprüfung oder die Darstellung des Datenbankinhalts sowohl eine qualitative als auch quantitative Investition erforderlich war.

Die KSV Wirtschaftsdatenbank unterliegt aufgrund ihres Aufbaues und der zu beziehenden Informationen dem § 18 Abs 2 Z 3 DSG 2000 iSd Vorabkontrolle durch die DSK. Aufgrund der Definition des § 4 Z 13 DSG 2000 ist sie jedoch kein Informationsverbundsystem da sie nicht „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 werden“ vorsieht. Die Informationen werden ausschließlich alleine vom KSV recherchiert, aufbereitet und der Datenbank tagesaktuell zugefügt. Hiefür bedient sich der KSV den unterschiedlichsten Informationsquellen wie zB des Grundbuches, Vereinsregisters, Inkassodaten, Bilanzen (Hinterlegung beim FBG), Firmenbucheinträge, Selbstauskünfte, Bankauskünfte und Gewerbeberechtigungsregister, etc. Die meisten Datenbanken sind „öffentliche Datenbanken“ und für jedermann einsehbar. Das schließt

³³⁷ OGH 4 Ob17/97x vom 11.2.1997

³³⁸ Blocher vergleicht es mit dem Leistungsschutzrecht zugunsten des Schallträgerherstellers iSd § 76 UrhG, JBl 1999, 34ff

schutzwürdige Geheimhaltungsinteressen im vornhinein aus. Inkassodaten werden aus dem eigenen Firmenbestand entnommen und sind durch § 94 Z 36 GewO gedeckt.

Bilanzinformationen werden vom KSV von den Firmenbuchgerichten herangezogen. Nach § 277ff UGB haben Kapitalgesellschaften ihre Jahresabschlüsse und den Lagebericht (eventuell auch noch den Corporate Governance-Bericht) beim jeweiligen Firmenbuchgericht (unter Androhung von Zwangsmaßnahmen und Strafbestimmungen gemäß § 283 UGB) zu hinterlegen.³³⁹ Dadurch besteht auch kein schutzwürdiges Geheimhaltungsinteresse an diesen Informationen iSd § 1 DSG 2000 welcher auch wirtschaftsbezogene Daten juristischer Personen mit einschliesst.

Eingearbeitete Bankauskünfte sind sowohl durch § 38 Abs 2 Z 6 BWG als Ausnahme von Bankgeheimnis als auch durch die Allgemeinen Geschäftsbedingungen der Banken (Z 25) gedeckt da die kontoführende Stelle unverbindlich und schriftlich allgemein gehaltene Bankauskünfte über Geschäftskunden an Geschäftskunden erteilen darf.

Bonitätsinformationen/-bewertungen sind Werturteile und unterliegen jedoch dem Schutzbereich des § 1 DSG 2000.

Darin enthaltene Ratingkennzahlen³⁴⁰ sind als Prognose einzustufen weil es über die Wahrscheinlichkeit der vertragsgemäßen Erfüllung von Liefer- und Leistungsverpflichtungen „urteilt“. Damit ist aber keine Garantie über den Eintritt eines bestimmten Erfolgs verbunden. Infolge des Prognosecharakters und der zukünftigen Unsicherheit ist dieses jedoch nicht als Tatsachenbehauptung zu qualifizieren und zum Zeitpunkt der Festsetzung als richtig oder falsch zu qualifizieren ist, dem Beweis nicht zugänglich. Sie sind deshalb als ein subjektives Werturteil, eine Meinungsäußerung über wie wirtschaftliche Bonität eines Unternehmens zu sehen und sind in dieser Hinsicht einer gerichtlichen Überprüfung in Hinblick auf die inhaltliche Richtigkeit, entzogen.³⁴¹

Wirtschaftsdaten von juristischen Personen sind ebenfalls personenbezogene Daten iSd § 1 DSG 2000. Ein schutzwürdiges Interesse ist in den meisten Fällen jedoch auszuschließen (abgesehen von Betriebs- und Geschäftsgeheimnissen), da eine allgemeine Verfügbarkeit besteht und der KSV diese Informationen nur sammelt, überprüft und dem jeweiligen

³³⁹ Bejahend OGH 28.6.2000, 6 Ob 162/00t = ÖJZ 2001/3 (EvBl); OGH 15.12.1999, 6 Ob 307/99m; OGH 9.3.2000, 6 Ob 5/00d; OGH 9.3.2000, 6 Ob 14/00b

³⁴⁰ Ausführlich hiezu *Niedostadek*, Rating, Rz 193ff

³⁴¹ *Duschanek in Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben, 299 der nur einen objektivierbaren Sachverhalt als „Daten“ bezeichnet; Einschätzungen oder Urteile sind keine Daten !

Datenbankeintrag zuordnet. Selbst dort wo eventuell schutzwürdige Geheimhaltungsinteressen des Betroffenen tangiert werden, sind diese nicht verletzt da überwiegend berechnigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. (§ 8 Abs 1 Z 4 DSG 2000)

Die Verarbeitung sowie die Übermittlung (zusammen „Verwendung“) solcher Daten iSd § 7 DSG 2000 ist durch die Gewerbeberechnigung iSd § 152 GewO gedeckt.

10.3. Die KKE (KonsumentenKreditEvidenz) Datenbank

Die KKE ist ein Präventionsinstrument, das über die Kreditsituation von Privatkunden informiert. Teilnehmer dieser Datenbank sind Kreditinstitute, Leasingunternehmen und Kredit gebende Versicherungsunternehmen, die sich verpflichtet haben, nicht nur Daten abzurufen sondern auch welche einzumelden. Nahezu alle Banken haben sich zur Teilnahme an der KKE entschlossen welche bereits seit 1964 besteht aber erst im Dezember 2007 als registriertes Informationsverbundsystem geführt wird. Eine Verbindung zur WKE (Warenkreditevidenz – siehe unten Kapitel 10.3.) besteht nicht. Jede Datenbank hat einen eigenen, geschlossenen Teilnehmerkreis und sonst hat niemand Zugang zu diesen Informationen.³⁴²

§ 8 Abs 1 Z 4 DSG 2000 stellt auf das überwiegende Interesse eines Dritten und nicht auf den unmittelbaren Empfänger ab und daher wird auch aufgrund der Rechts- und Aufgabenstellung der Banken und ihre Funktion in der Volkswirtschaft, eine Weiterleitung von Daten an eine Evidenzstelle zulässig sein.³⁴³

Der KSV ist datenschutzrechtlicher Betreiber (Dienstleister iSd § 4 Z 5 DSG 2000) der KKE und in dieser Funktion zentrale Auskunftsstelle für Betroffene. Die notwendige Hard- und Software wird von

First Data Austria GmbH

Floridsdorfer Hauptstrasse 1, 1210 Wien

FN 54456h (= Subdienstleister iSd §§ 4 Z 5 und 11 Abs 1 Z 3 DSG 2000), bereitgestellt.

³⁴² aA Stadler, Wirtschaftsinformationen, 16 der aufgrund der Beschränkung der gesetzlichen Anordnung einer Großkreditevidenz (damals § 16 KWG nunmehr § 75 BWG) auf eine prinzipielle Unzulässigkeit einer Kleinkreditevidenz schließt.

³⁴³ Heller, Kreditwesengesetz (1979), 14; Schäffer, Wirtschaftsaufsicht, ÖZW 1978, 37ff, 65 ff; Duschanek Datenschutzgesetz in Ruppe (Hrsg), Geheimnisschutz im Wirtschaftsleben, 313

Die Datenbank weist folgenden Umfang aus (per Stichtag 31.12.2007)

Personendaten	2.868.416	ca. 2.300.000 (2003)
Anzahl der Kredite	4.052.573	
Personen mit Negativa	185.972	
Zahlungsanstände	524.479	
Jährliche Anfragen b. KSV	3.726.400	ca. 2.700.000 (2003)
Selbstauskünfte	42.052	
Teilnehmer	1.012*	

*) Aktive Kreditgeberleitzahlen

Dadurch kann sichergestellt werden, dass Konsumenten nicht bei unterschiedlichen Instituten Kredite aufnehmen, die sie nicht mehr rückführen können. Sie dient einerseits natürlich zum Schutz vor Ausfällen bei den teilnehmenden Unternehmungen, andererseits auch dem Konsumenten als Selbstschutz vor Überschuldung.³⁴⁴

Die KKE Anfrage zeigt den einzelnen Fall mit Kredithöhe bzw. Rahmen, den Beginn der Laufzeit, die voraussichtliche Endfälligkeit und die Rückzahlungsvereinbarung. Sie informiert weiters, ob ein Kredit vereinbarungsgemäß bezahlt wird, bzw. liefert Negativinformationen bei Fälligstellungen, Klagsführung, etc. Jeder Konsumentenkredit wird gemäß den Richtlinien zwischen Auftraggebern und KSV eingemeldet (inkl. Mitverpflichtete).

Folgende Zahlungsanstände werden eingemeldet:

- 3. Mahnung (Symbol **3M**)
- Fälligstellung (Symbol **FS**)
- Klage (Symbol **KL**)
- Exekution (Symbol **EX**)
- Ausbuchung (Symbol **AB**)
- (- Uneinbringlich [Symbol **UE**])

Die Löschung erfolgt bei

- Krediten ohne Zahlungsanstände – nach Laufzeitende

³⁴⁴ Infobroschüre des KSV

- Krediten mit Zahlungsanständen

- 5 Jahre nach vollständiger Tilgung
- 7 Jahre nach Teiltilgung

Am unten angeführten Musterbeispiel lässt sich sehr leicht die fast nahtlose Überprüfung jeder Privatperson und Firma(Unternehmen) welche sich in Österreich um einen (Waren-)Kredit, Leasing, etc. bemüht, nachvollziehen:³⁴⁵

³⁴⁵ Siehe weiters die Ausführungen von *Appl*, Der gläserne Schuldner, NZ 2007,44 wo über die Vorarbeiten zur Schaffung eines Mobiliarpfandregisters im Verhältnis zum Datenschutz ausführlich referiert wird

Willkommen auf der KKE Homepage!

KSV-KonsumentenKreditEvidenz: Kompetenz seit 40 Jahren

Vorteile

- Rasche Kreditentscheidungen mittels Online-Bonitätsprüfung
- Auch am Samstag abrufbar
- Einfache übersichtliche Benutzeroberfläche
- Keine Programmierung seitens Ihrer Bank notwendig
- Direkte Bearbeitung des Kreditfalles online

Login ?

Identifikation:

Passwort:

Benutzerkennung:

Filialnummer: ?

Login

Systemverfügbarkeit

Montag bis Mittwoch 7:00 - 20:00 Uhr

Donnerstag und Freitag 7:00 - 21:00 Uhr

Samstag 7:00 - 20:00 Uhr

Hotline

Bei Fragen zum Web erreichen Sie uns unter 01/534 94 DW 200 Montag bis Freitag in der Zeit von 8.00 Uhr bis 16.00 Uhr.

KKE Hauptmenü

Obligo ? ▶ Bonitätsüberprüfung	Mitteilungen ? Gewährung... ▶ offene Kreditanfrage ▶ offene Aufstockung Ablehnung... ▶ offene Kreditanfrage ▶ offene Aufstockung Mitteilung zu... ▶ gewährtem Kredit Rückzahlung... ▶ gewährter Kredit Storno... ▶ Storno	Mitverpflichtete ? ▶ Entlassen ▶ Hinzufügen ▶ Austauschen
Kreditanfragen ? ▶ Offene Kreditanfrage ▶ Offene Aufstockung ▶ Kreditanfrage mit gleichzeitiger Gewährung ▶ Aufstockung mit gleichzeitiger Gewährung		Personendaten ? ▶ Namensänderung ▶ Adressänderung

Ergebnis Bonitätsüberprüfung

Abgefragte Person

KKE-Nummer	4697
Familienname	TEST
Vorname	TESTI
Geburtsdatum	14.04.1944
Adresse	TESTWEG 121
Land-PLZ Wohnort	A-1010 WIEN
Frühere Adresse	MUSTERGASSE 2/3/4
Früheres Land-PLZ Wohnort	A-1220 WIEN

Ihre rückbezahlte gewährte Kreditaufstockung

Kreditkontonummer	167321
Lfd. Kreditnummer	9169
Kreditart	Leasingvertrag EUR
Kredithöhe	110.000
Laufzeit	72 Monate
Rate / Höhe	monatlich ab 22.06.2007
Dat. Endfälligkeit / Kreditende	22.06.2013
Kreditzustand	Kredit-Aufstockung
Datum der Gewährung	22.06.2007
Datum der Rückzahlung	17.06.2008
Ausfallbürge ist	WIESINGER REINI, geb. am 02.02.1915
Haftungsbetrag	60.000

Ihr rückbezahlter Kredit

Kreditkontonummer	1224
Lfd. Kreditnummer	1
Kreditart	Abstattungskredit EUR 350.000
Kredithöhe	
Laufzeit	25 Monate
Rate / Höhe	vierteljährlich ab 05.04.2007
Dat. Endfälligkeit / Kreditende	21.07.2009
Kreditzustand	Kredit
Datum der Gewährung	05.04.2007
Datum der Rückzahlung	05.07.2007
1.Negativeintrag / Datum	Klage eingreicht 14.06.2007
2.Negativeintrag / Datum	Exekution eingereicht 21.06.2007
3.Negativeintrag / Datum	Fälligstellung 01.06.2007
Ausfallbürge ist	MAIERKSV THOMAS, geb. am 20.02.1940

Ihr gewährter Kredit

Kreditkontonummer	83470897
Lfd. Kreditnummer	1
Kreditart	Abstattungskredit EUR 120.000
Kredithöhe	
Laufzeit	120 Monate
Rate / Höhe	vierteljährlich ab 15.11.2007
Dat. Endfälligkeit / Kreditende	14.11.2017
Kreditzustand	Kredit
Datum der Gewährung	31.10.2007
Wechselbürge ist	HUEPFER GMBH
Firmenbuchnummer	55599H

Ihr offen angefragte Kreditaufstockung

Kreditkontonummer	83470897
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Abstattungskredit EUR 130.000
Laufzeit	120 Monate
Rate / Höhe	vierteljährlich
Dat. Endfälligkeit / Kreditende	17.06.2018
Kreditzustand	Offene Anfrage für eine Kreditaufstockung

Wechselbürge ist	HUEPFER GMBH
Firmenbuchnummer	55599H

Ihr gewährter Kredit

Kreditkontonummer	12345
Lfd. Kreditnummer	9192
Kreditart Kredithöhe	Abstattungskredit EUR 20.000
Laufzeit	120 Monate
Rate / Höhe	halbjährlich ab 01.08.2007
Dat. Endfälligkeit / Kreditende	01.08.2017
Kreditzustand	Kredit
Datum der Gewährung	10.07.2007

Ihre Ablehnung offene Kreditaufstockung

Kreditkontonummer	12345
Lfd. Kreditnummer	9192
Kreditart Kredithöhe	Abstattungskredit EUR 45.000
Laufzeit	180 Monate
Rate / Höhe	halbjährlich ab 18.06.2008
Dat. Endfälligkeit / Kreditende	18.06.2023
Kreditzustand	Ablehnung offene Kredit-Aufstockung
Datum der Ablehnung	Vom Kunden zurückgezogen 15.06.2008

Ihr gewährter Kredit

Kreditkontonummer	986896
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Abstattungskredit EUR 45.000
Laufzeit	60 Monate
Rate / Höhe	monatlich ab 05.05.2007
Dat. Endfälligkeit / Kreditende	05.05.2012
Kreditzustand	Kredit
Datum der Gewährung	05.05.2007
Mitschuldner ist	ADVENT KRANZ, geb. am 09.09.1990
Haftungsbetrag	45.000 ab 05.05.2007

Ihre gewährte Kreditaufstockung

Kreditkontonummer	2893576
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Abstattungskredit EUR 75.000
Laufzeit	120 Monate
Rate / Höhe	monatlich ab 18.06.2008
Dat. Endfälligkeit / Kreditende	18.06.2018
Kreditzustand	Kredit-Aufstockung
Datum der Gewährung	18.06.2008

Offen angefragter Kredit

Kreditart Kredithöhe	Leasingvertrag EUR 47.110
Laufzeit	36 Monate
Rate / Höhe	monatlich
Dat. Endfälligkeit / Kreditende	26.11.2010
Kreditzustand	Offene Anfrage
Datum der Anfrage	26.11.2007

Offen angefragter Kredit

Kreditart Kredithöhe	Leasingvertrag EUR 61.200
Laufzeit	36 Monate
Rate / Höhe	monatlich
Dat. Endfälligkeit / Kreditende	04.12.2010
Kreditzustand	Offene Anfrage
Datum der Anfrage	04.12.2007

Offen angefragter Kredit

Kreditart Kredithöhe	Leasingvertrag EUR 41.641
Laufzeit	36 Monate
Rate / Höhe	monatlich
Dat. Endfälligkeit / Kreditende	18.02.2011
Kreditzustand	Offene Anfrage
Datum der Anfrage	18.02.2008

Ihre Ablehnung offene Kreditanfrage

Kreditkontonummer	98275
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Leasingvertrag EUR 12.308
Laufzeit	36 Monate
Rate / Höhe	monatlich ab 09.06.2008
Dat. Endfälligkeit / Kreditende	09.06.2011
Kreditzustand	Ablehnung offene Anfrage
Datum der Ablehnung	Mangelnde Bonität 09.06.2008

Ihre gewährte Kreditaufstockung

Kreditkontonummer	786905
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Abstattungskredit EUR 10.000
Laufzeit	120 Monate
Rate / Höhe	monatlich ab 18.06.2008
Dat. Endfälligkeit / Kreditende	18.06.2018
Kreditzustand	Kredit-Aufstockung
Datum der Gewährung	15.06.2008
Ausfallbürge ist	NOVAKKE SUSA, geb. am 24.04.1940

Ihr gewährter Kredit

Kreditkontonummer	31498714
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Hypothekarkredit EUR 450.000
Laufzeit	120 Monate
Rate / Höhe	monatlich ab 20.06.2007
Dat. Endfälligkeit / Kreditende	20.06.2017
Kreditzustand	Kredit
Datum der Gewährung	20.06.2007
Bürge für	SCHMIDKE LISA, geb. am 17.07.1977

Ihre gewährte Kreditaufstockung

Kreditkontonummer	32343
Lfd. Kreditnummer	1
Kreditart Kredithöhe	Abstattungskredit EUR 150.000
Laufzeit	240 Monate
Rate / Höhe	monatlich ab 21.11.2007
Dat. Endfälligkeit / Kreditende	21.11.2027
Kreditzustand	Kredit-Aufstockung
Datum der Gewährung	20.11.2007
Wechselbürge für	WAGNERKKE HANS PETER, geb. am 29.04.1975

Ende des Dokuments

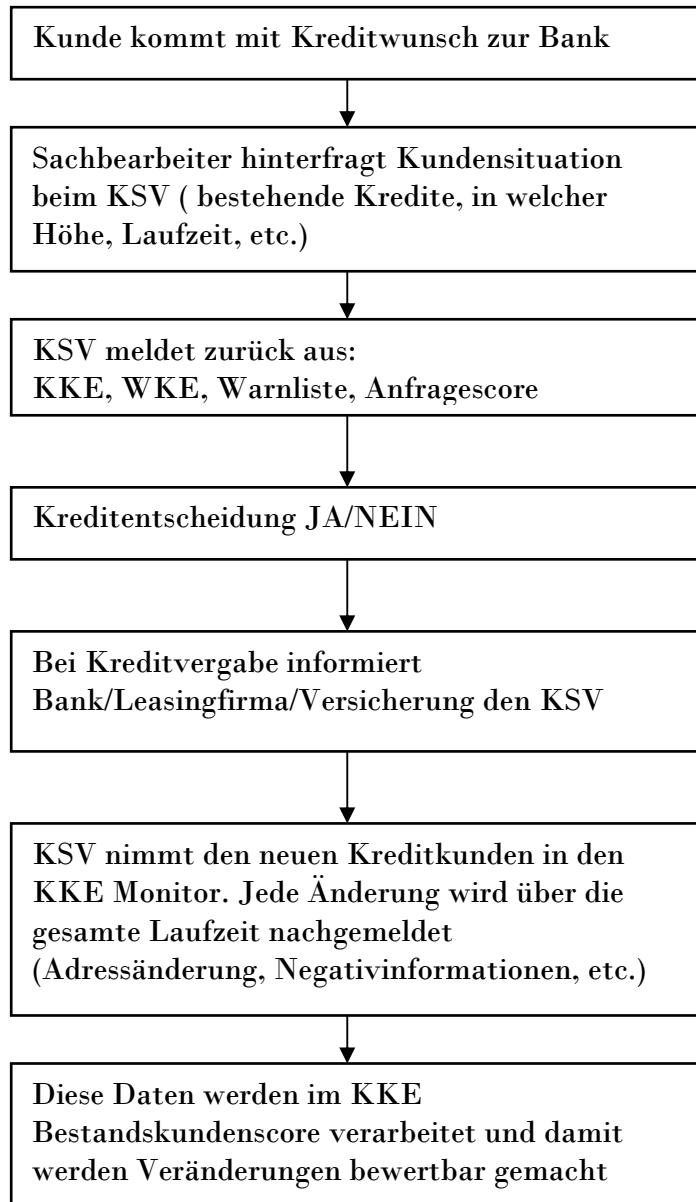
Hauptmenü
[[Seitenanfang](#)]

Hilfe bei Problemen finden Sie unter KKE_Web@ksv.at oder 050 1870 DW 1102.

2

[AGB](#) | [Impressum](#) | [Downloads](#)

Anbei das Ablaufdiagramm wie die Prüfung eines zukünftigen Kreditnehmers vor Ort und beim KSV im Hintergrund abläuft:



Es wird unterschieden zwischen dem KKE Anfragescore und dem KKE Bestandskundenscore. Erster gibt die Wahrscheinlichkeit eines möglichen Forderungsausfalls zum Zeitpunkt einer Kreditanfrage an. Zweiter zeigt die Ausfallwahrscheinlichkeit aufgrund einer permanenten Bonitätsüberwachung bestehender Privatkunden und ermöglicht eine aktuelle Risikoklassifizierung.

KKE Anfragescore	KKE Ratingklasse	Ausfallwahrscheinlichkeit
0 – 310	A	Sehr gering
311 – 430	B	
431 – 483	C	Gering
484 – 543	D	
544 – 607	E	Mittel
608 – 680	F	
681 – 773	G	Erhöht
774 – 835	H	Hoch
836 – 869	I	
870 – 889	J	
890 – 917	L	Sehr hoch
918 – 999	M	

Das Kreditscoring greift auf anonymisierte Krediterfahrungen aller Daten aller Kunden aus der Vergangenheit zurück.

Bedeutende Einflussfaktoren für das Ausfallrisiko sind:

- Alter des Kreditnehmers
- Anzahl der Kreditfinanzierungen
- Anzahl der Kreditinstitute
- Wohnregion
- Häufigste Kreditart
- Anzahl der Kredit im letzten Jahr
- Restlaufzeiten
- Negativmerkmale (3. Mahnungen, Fälligstellungen,...)³⁴⁶

³⁴⁶ KSVWerbefolder – Mit dem KSV zur Kreditentscheidung

10.3.1. Rechtliche Beurteilung

Die KSV Kleinkreditkatasterevidenz (KKE) Datenbank unterliegt aufgrund ihres Aufbaues und der zu beziehenden Informationen dem § 18 Abs 2 Z 3 DSG 2000 iSd Vorabkontrolle durch die DSK. Aufgrund der Definition des § 4 Z 13 DSG 2000 ist sie auch ein Informationsverbundsystem da sie „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 werden“ vorsieht. Der KSV agiert jedoch nur als betreibende Plattform im Sinne eines Dienstleisters nach §§ 4 Z 5 bzw 50 DSG 2000 und ist auch erste Anlaufstelle für Auskünfte und dergleichen.

Bei den eingemeldeten Daten handelt es sich um zwar nicht um sensible Daten iSd § 4 Z 2 DSG 2000 jedoch zum Großteil um personenbezogene Daten welche die schutzwürdigen Geheimhaltungsinteressen der Betroffenen iSd § 1 DSG 2000 tangieren und welche dazu geneigt sind, Tatsachen aus dem höchstpersönlichen Lebensbereich des Betroffenen zu enthüllen und ihn aus der Sicht Dritter herabzusetzen und sein Ansehen untergraben zu können.³⁴⁷

Wie jedoch bereits eingangs angeführt, stellt § 8 Abs 1 Z 4 DSG 2000 auf das überwiegende Interesse eines Dritten und nicht auf den unmittelbaren Empfänger ab. Die Datenbank kann aufgrund des geschlossenen Benutzerkreises (nur Banken und Leasingunternehmen) als „nicht öffentlich zugängliche“ Datenbank tituiert werden und daher wird auch aufgrund der Rechts- und Aufgabenstellung der Banken und ihrer Funktion in der Volkswirtschaft, eine Weiterleitung von Daten an eine Evidenzstelle zulässig sein.³⁴⁸ Die DSK erteilte hiezu auch einen Genehmigungsbescheid.³⁴⁹

§ 39 BWG regelt die allgemeine Sorgfaltsverpflichtung der Kreditinstitute sowie § 25c KschG die Aufklärungspflicht im Falle der Interzedenteninvolvierung worauf im weiteren Sinn auf die Notwendigkeit einer ordentlichen Bonitätsprüfung geschlossen werden kann.

³⁴⁷ Dohr-Pollirer-Weiss, Datenschutzrecht² (2002), § 33 Rz 3 f

³⁴⁸ Siehe FN 343

³⁴⁹ GZ K600.033-018/0002-DVR/2007 vom 12.Dezember 2007

Auch spricht die Verbraucherkredit-RL 2008/48/EG in Erwägungsgrund 26 von der Ergreifung von „geeigneten Maßnahmen der Mitgliedsstaaten zur Förderung verantwortungsvoller Verfahren in allen Phasen der Kreditvergabe“. Zu diesen Maßnahmen gehört die Unterrichtung und Aufklärung der Verbraucher, einschließlich Warnungen vor dem Risiko des Zahlungsverzuges oder der Überschuldung. Weiters sollen Kreditgeber dafür verantwortlich sein, in jedem Einzelfall die Bewertung der Kreditwürdigkeit des Verbrauchers zu prüfen. Zu diesem Zweck sollten sie nicht nur die vom Verbraucher im Rahmen der Vorbereitung des betreffenden Kreditvertrags, sondern auch die während einer schon länger bestehenden Geschäftsbeziehung erteilten Auskünfte heranziehen dürfen. Gemäß Art 8 der RL besteht von Seiten der Kreditgeber die Verpflichtung die Kreditwürdigkeit/Bonität der potentiellen Kreditnehmer/Verbraucher zu überprüfen. Dies kann anhand von Informationen des Verbrauchers als auch mit Hilfe einer Datenbank geschehen. Nach Art 9 Abs 2 der RL hat der Kreditgeber den Verbraucher unverzüglich und unentgeltlich bei einer negativen Entscheidung über das Ergebnis dieser Abfrage und über die Angaben der betreffenden Datenbank zu unterrichten, es sei denn, dass die Unterrichtung nach anderen gemeinschaftsrechtlichen Vorschriften nicht zulässig wäre oder Zielen der öffentlichen Ordnung oder der öffentlichen Sicherheit zuwider läuft.

Auch der EuGH geht in seiner Entscheidung *Asnef-Equifax/Ausbanc*³⁵⁰ von der Zulässigkeit der Existenz von Systemen zum Austausch von Kreditinformationen aus weil sie die „Ungleichheit des Informationsstands von Gläubiger und Schuldner verringern, was die Vorhersehbarkeit der Rückzahlungswahrscheinlichkeit verbessert. Damit sind diese grundsätzlich geeignet, die Ausfallquote von Kreditnehmern zu verringern und dadurch den Wirkungsgrad des Kreditangebots“.

Die Frage der rechtlichen Zulässigkeit dieser Datenbank steht daher in meinen Augen außer Frage.

³⁵⁰ EuGH 23.11.2006, C-238/05, Rn 46,47 =ÖBA 2007/27 (EuGH)

10.4. EXKURS: Sonderfall Grosskreditevidenz ³⁵¹

Meldungen über Forderungen mit einem Rahmen von mehr als € 350.000 sind an die Oesterreichische Nationalbank (OeNB) zu melden und zwar bei

- Abschluss von Geldkreditverträgen und die Gewährung von Gelddarlehen (Kreditgeschäft);
- Kauf von Schecks und Wechseln, insbesondere die Diskontierung von Wechseln (Diskontgeschäft)
- Übernahme von Bürgschaften, Garantien und sonstigen Haftungen für andere, sofern die übernommene Verpflichtung auf Geldleistungen lautet (Garantiegeschäft);
- der Entgegennahme von Bauspareinlagen und die Vergabe von Bauspardarlehen nach dem Bausparkassengesetz (Bauspargeschäft);
- Abschluss von Leasingverträgen (Leasinggeschäft);

Diese Meldungen sind in § 75 BWG vorgeschrieben und daher auch nach § 8 Abs Z 1 DSG 2000 zulässig.

Diese gesetzliche Verpflichtung stellt eine Ausnahme von der Pflicht zur Wahrung des Bankgeheimnisses dar obwohl sie nicht extra in § 38 BWG normiert ist. Sofern in § 75 BWG nicht eine Verletzung der Verfassungsbestimmung des § 1 DSG 2000 gesehen wird, steht die Meldung der Großkredite nicht in Widerspruch zur Grundrechtsnorm.

Meldungen an eine Evidenzstelle über andere als die Großkredite des § 75 BWG, sind gesetzlich nicht vorgeschrieben und es auch fraglich ist ob sie zur Wahrung überwiegender berechtigter Interessen Dritter dienen. Dies macht die explizite Einholung einer ausdrücklichen Zustimmungserklärung des Betroffenen notwendig da ansonsten mit solch einer Meldung es zur Verletzung des Bankgeheimnisses iSd § 38 BWG kommen würde.³⁵²

Diese Meldung die weit über eine allgemein gehaltene Bankauskunft hinausgeht, wird auch anderen Banken und Unternehmen der Vertragsversicherung unter Angabe der Gesamthöhe der eingeräumten Kredite und der Namen der diversen Kreditgeber (§ 75 Abs 5 BWG) auf Anfrage von der Nationalbank zur Verfügung gestellt. Im Wortlaut von § 38 Abs 4 BWG wurde die Änderung von § 75 Abs 3 auf § 75 Abs 5 BWG nicht berücksichtigt.

³⁵¹ Aus thematischen Gründen kann nicht genauer darauf eingegangen werden

³⁵² Bejahend *Duschaneck*, Geheimnisschutz 312f; *Potyka*, Datenschutz in der Wirtschaft, 137ff

10.5. Die UKV Datenbank – Liste der Unerwünschten KontoVerbindungen

In dieser Liste vermerken Banken Informationen über Kunden, die ihren Verpflichtungen – z.B. Rückzahlung eines Kredites, Abdeckung eines Girokontos – nicht nachkommen oder aber auch bei der unerlaubten Verwendung von Bankomat- und Kreditkarten. Diese „Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten“ steht den Banken, Leasingfirmen und Gläubigerschutzverbänden über ein Informationsverbundsystem zur Verfügung.

Wer einmal auf dieser Liste aufscheint, hat danach sehr stark eingeschränkte Möglichkeiten mit einer der teilnehmenden Banken/Leasingfirmen in Geschäftsbeziehung zu treten. Sollte es trotzdem zu einer Geschäftsbeziehung kommen bzw schon eine vorhanden sein, so wird die Bank die (weitere) Geschäftsbeziehung so gestalten, dass jegliches Risiko für die Bank ausgeschaltet wird. Dadurch wird der Kunde gleichzeitig natürlich auch davon abgehalten sich weiter finanziell zu belasten was jedoch unten den oben angeführten Tatsachen als eine Art Reflexwirkung angesehen werden kann. Altruistische Motive standen bei der Schaffung der Negativliste allerdings nicht Pate.³⁵³

In Österreich gibt es ca. 12.000 Personen welche aufgrund Aufscheinens in der UKV-Liste kein Bankkonto besitzen. Ausweg gibt es seit kurzem durch die Eröffnung und Einrichtung von Bankkonten für diese Personengruppen bei der „Zweiten Sparkasse“.³⁵⁴ Die Eintragung von Daten von Betroffenen in die Warnliste ist eine öffentlich zugängliche Verwendung iSd § 33 Abs 1 DSG 2000.

Der KSV fungiert hier nur als „Plattform“ für die Führung und Wartung der UKV Liste und ist daher Dienstleister aber auch erste Kontaktstelle für diesbezügliche Informationen für Betroffene.³⁵⁵ Die einmeldende Bank jedoch welche über Einmeldung, Veränderung und Löschung entscheidet und daher die „Datenhoheit“ besitzt, ist Auftraggeber und daher passiv legitimiert zur Löschung iSd § 27 DSG 2000.

Im Zuge des Prüfverfahrens der DSK zur Führung dieses Informationsverbundsystems waren folgende datenschutzrechtlichen Defizite hervorgekommen:

³⁵³ Krasensky, Kreditschutz im Privatkundengeschäft, ÖBA 1965, 247ff

³⁵⁴ A. Müller, Der Standard, 26.11.2007

³⁵⁵ Weissel bezeichnet den KSV auch als Rechtsträger iSd § 1 Abs 5, EDVuR 1990, 62; dazu VfGH 12.10.1989, G 238-241/88, V 209-212/88; Dohr/Pollirer-Weiss, DSG, Anm 4 zu § 17 DSG

- Mangelnde Information der Betroffenen darüber, wann und aus welchen Anlässen Daten in die „Warnliste“ aufgenommen werden
- Mangelnde Information der Betroffenen darüber, wer Auftraggeber bzw. Beauftragter des Auftraggebers im Hinblick auf die Bearbeitung von Überprüfungs- und Löschungsbegehren ist
- Mangelnde Transparenz über die Rechtsgrundlagen und die Regeln zur Führung dieser Dateien besonders im Hinblick auf angemessene Löschungsfristen
- Keine ausreichende Meldung im Datenverarbeitungsregister (DVR); teilnehmende Kreditinstitute wurden ersucht eine Meldung als Auftraggeber abzugeben

Datenanwendungen welche gemäß § 18 Abs 2 DSG 2000 der Vorabkontrolle unterliegen, können, wenn es wenn zur Wahrung der geschützten Interessen der Betroffenen notwendig ist, aufgrund der Ergebnisse des Prüfverfahrens durch die DSK Auflagen für die Vornahme der Datenanwendung erteilt und durch Bescheid zugestellt werden.

(§ 21 Abs 2 DSG 2000)

Dies hatte zur Folge, dass teilnehmende Bankengruppen (insbesondere die Raiffeisengruppe) mehrere hundert Meldungen einbringen mussten, nämlich für jede Bankgesellschaft oder – genossenschaft eine eigene.³⁵⁶ Die DSK hat anlässlich der empfehlungsgemäßen Erstattung der Meldung an das DVR seitens der involvierten Kreditinstitute mit Bescheid³⁵⁷ die Rahmenbedingungen für die Führung der „Warnliste“ im Detail festgelegt:

- Die Eintragung von Daten darf ausschließlich nur aus den im Bescheid bezeichneten Anlässen erfolgen
- Die Pflicht zur Information des Betroffenen anlässlich der Eintragung in die Warnliste nach dem Grundsatz von Treu und Glauben
- Festlegung der Maximaldauer der Eintragung in die Warnliste nach Schuldtilgung von 7 Jahren bzw. von 3 Jahren nach vollständiger Bezahlung
- Einrichtung einer Auskunft- und Beschwerdestelle beim KSV

³⁵⁶ Knyrim, Datenschutzrecht, 23 (FN 49)

³⁵⁷ GZ K095.014/016-DSK 2001 und GZ K095.014/021-DSK 2001 vom 23. November 2001; der Bescheidtext kann unter www.ris.bka.gv.at abgefragt werden

- Aufgrund des Vorliegens überwiegender berechtigter Interessen an der Führung einer derartigen Warnliste zum Zweck der Risikominimierung bei der Kreditvergabe und zum Zweck des Gläubigerschutzes,

werde die Registrierung der Warnliste nicht untersagt.

Die Einhaltung der durch Bescheid festgelegten Auflagen ist im Übrigen durch folgende Sanktionen abgesichert:

1. Bei Zuwiderhandeln kann von der Bezirksverwaltungsbehörde (BVB) eine Verwaltungsstrafe gemäß § 52 Abs 1 Zi 3 DSG 2000 bis zu € 18.890 verhängt werden
2. Bei vorgesetzten Verstößen gegen den Auflagenbescheid kann die DSK das Registrierungsverfahren neu aufrollen und die Fortführung der Datenverarbeitung untersagen³⁵⁸

Wie bereits oben erwähnt, würde die Meldung an eine Evidenzstelle, dass Kreditverpflichtungen nicht nachgekommen wird oder Bankomat- und/oder Kreditkarten missbräuchlich verwendet werden ohne Vorliegen einer Zustimmungserklärung einen Verstoß gegen das Bankgeheimnis iSd § 38 BWG bedeuten. Diese Zustimmungserklärung bedeutet sodann gleichzeitig die Zulässigkeit nach §§ 1 und 7, 8 DSG 2000.

*Weissel*³⁵⁹ stimmt dem insoweit zu als auch ein rechtswidrig agierender Kunde seinen Geheimhaltungsanspruch nicht verliert was § 23 Abs 1 Z 5 KWG (nunmehr § 38 Abs 2 Z 7 BWG) zeigt, der die Bank zur Offenbarung von Kundengeheimnissen ermächtigt sofern dies zur Klärung von Rechtsangelegenheiten zwischen Kunden und Kreditinstitut notwendig ist.

Der Umkehrschluss daraus, wonach die Bank in diesen Fällen Dritten gegenüber zur Verschwiegenheit verpflichtet ist, lässt sich daraus in seinen Augen jedoch nicht schließen, da § 23 Abs 2 KWG (nunmehr § 38 Abs 2 BWG) keine abschließende Aufzählung jener Fälle enthält, in welchen die Verschwiegenheitspflicht der Bank entfällt.

Würde sodann ein betroffener Kunde seine Zustimmungserklärung widerrufen, so ist diese jedoch zu beachten. Eine Datenweitergabe darf jedoch dennoch erfolgen, da anstatt der Zustimmung iSd § 8 Abs 1 Z 2 DSG 2000 der Grund der überwiegenden berechtigten

³⁵⁸ DSB 2001, 19ff

³⁵⁹ *Weissel*, Das Bankgeheimnis in der österreichischen Grundrechtsordnung, ÖZW 1989, 80ff (81ff)

Interessen des Auftraggebers iSd § 8 Abs 1 Z 4 DSG 2000 tritt und das Interesse des Kreditinstituts weitaus höher zu bewerten ist als jenes der Weitergabe der Informationen des Betroffenen. Gleichzeitig ist jedoch unter der Prämisse des Gläubigerschutzes eine Übermittlung nur gerechtfertigt, wenn die die betreffenden Daten zuverlässig und objektivierte Aussagen über die mangelnde Kreditfähigkeit oder –würdigkeit des Betroffenen beinhalten.³⁶⁰ Dieses Prinzip lässt sich insbesondere aus der ergangenen OGH Entscheidung³⁶¹ zu § 1330 ABGB ableiten wo einem Gläubigerschutzverband keine Fahrlässigkeit vorgeworfen werden kann wenn er den Namen eines Schuldners in seinen Aussendungen nennt gegen den Fahnisexekution geführt wird. Wobei idR davon ausgegangen werden kann, dass Exekutionen Zahlungsunfähigkeit indizieren.³⁶²

Unstrittig sind danach jedenfalls jene Fälle, wo das angestrengte Exekutionsverfahren nicht zur Hereinbringung der Forderung geführt hat oder ein Insolvenzverfahren zwischenzeitlich eröffnet wurde bzw mangels Masse abgewiesen wurde.

Liegt diesbezüglich keine titulierte Forderung vor, so kommt es auf die Umstände des Einzelfalles an, wobei zugunsten des Betroffenen festgehalten werden muss, dass eine objektive Verifizierung über die Richtigkeit des geltend gemachten Anspruchs fehlt und der Empfänger der (Negativ-)Information keine Klarheit darüber hat ob nicht berechtigte Einwendungen dagegen erhoben wurden.

Auch die Bankgeheimnisbestimmungen stehen einer Meldung nicht entgegen, da zwar die einmal gegebene Zustimmungserklärung ausreichend und der Widerruf iSd § 8 Abs 1 Z 2 DSG 2000 beachtlich ist aber anstatt dieses Übermittlungsgrundes nun § 8 Abs 1 Z 4 DSG 2000 zu Tage tritt. Bei Vorliegen überwiegender berechtigter Interessen Dritter ist daher auch keine Verletzung schutzwürdiger Interesses des Täters/Betroffenen zu sehen.³⁶³

Anlässlich der Registrierung der UKV-Warnliste wurde jedem teilnehmenden Auftraggeber die Auflagen gemäß § 21 Abs 2 DSG 2000 für die Vornahme der Datenanwendung durch Bescheid erteilt.

Eine Liste aller teilnehmenden Banken war nicht zu bekommen jedoch würde die auch zu lange ausfallen weil sich die Zahl um die 750 beläuft. Zusammengefasst kann gesagt werden,

³⁶⁰ Stadler, Wirtschaftsinformationen und Datenschutz, 12; Feuerborn in *Sichtermann-Feuerborn-Kirchherr-Terdenge*, Bankgeheimnis und Bankauskunft, 444

³⁶¹ OGH 20.10.1987 4 Ob 338/87, wbl 1988, 99ff

³⁶² OGH 08.05.1984 4 Ob 559/83 = SZ 57/87 = EvBl 1985/92, 461 = JBl 1985,494 = RdW 1984,242

³⁶³ So schon Potyka, Datenschutz in der Wirtschaft, 138ff zu § 18 DSG 1978; Pruckner, Datenschutz im Kreditwesen 147

dass alle Banken und Sparkassen in Österreich welche über eine Bankleitzahl (BLZ) verfügen in diese Liste einmelden. Als Informationsverbundsystem besteht diese Datenbank seit 2001.

Im Jahr 2007 befanden sich ca. 427.000 Datensätze in dieser Datei was ungefähr 250.000 bis 300.000 Einzelpersonen entspricht.

Einmeldekriterien: Alle teilnehmenden Institute melden direkt an die
BA-CA Administration Services Gmbh, Julius Tandler Platz 3, 1090 Wien
Handelsgericht Wien, FN 91507 w, UID 61234701 ein
(= Subdienstleister iSd § 11 Abs Z 3 DSG 2000)

Privatpersonen werden in folgenden Fällen in die Warnliste aufgenommen:

- Bankomat,- Kreditkarten- und (früher) Scheckkartenmissbrauch (Symbol **NEG**)
- Fälligstellung bzw. Rechtsverfolgung nach qualifiziertem Zahlungsverzug bei
 - o Girokonten (Symbol **G**)
 - o Krediten (Symbol **K**)
 - o Kreditkarten (Symbol **C**)
- Generelle Aufkündigung einer Kontoverbindung durch die Bank (Symbol **AUF**)
- Zahlungsanstände in Zusammenhang mit einer Bürgschaft (Symbol **B**)
- Versuchter Betrug (Symbol **VBG**)

Der Betrag wird nun in € 1.000er Schritten (früher öS 10.000er Schritte) nach dem Symbol angezeigt. So bedeutet zB K04 größere Zahlungsanstände in Zusammenhang mit einem Kredit(-konto) in der Höhe zwischen € 3.001 und € 4.000. (früher zwischen öS 30.001 und öS 40.000). K99 würde in diesem Fall (und auch in den anderen Fällen) den maximal möglichen Betrag größer € 100.000 darstellen.

Automatische Löschungen erfolgen in regelmäßigen Abständen nach Abdeckung der offenen Forderung:

- idR drei Jahr nach vollständiger Bezahlung
- idR sieben Jahre nach erfolgter Teilzahlung

Ein Datensatz ist folgendermaßen aufgebaut (abhängig von der jeweiligen technischen Umsetzung beim Teilnehmer):

ID.Nr., Negativsymbol, UKV Datum, Status, First Name, Last Name, Birthday, Bank Account Nr., Bank Code, Address, City, Zip Code, Reference Number

Beispiel:³⁶⁴

1234567 K99 02/08 E Max Mustermann 19.01.01 123456789 11111 Mustermannstrasse 1 1010 Wien 98765432

Status-Anzeigen:

E= Erstmeldung

A= Änderung

S= Stornierung

Ebenso wird pro Kontonummer eine so genannte Referenznummer seitens der Bank vergeben. Wenn es dann zu einem Eintrag eine Änderung gibt, dann sollte dieselbe ID-Nummer ersichtlich sein, damit man weiß zu welchem Eintrag diese Änderung/Löschung gehört.

10.5.1. Das OGH Urteil 6 Ob 275/05t vom 15.12.2005

Nach einer relativ neuen und grundlegenden Entscheidung des Obersten Gerichtshofs (OGH) dürfen Banken ihre Kunden nicht ohne konkrete Vorwarnung auf diese Liste setzen weil sie sonst schadenersatzpflichtig werden. Ein Urteil des LG Bonn³⁶⁵ welches sowohl die Kündigung eines Kredites und auch Meldung an die SCHUFA³⁶⁶ nur aufgrund von „weichen Bonitätsdaten“ (= Negativdaten ohne gerichtliche Verurteilung) als unzulässig ansah, spiegelt sich in meinen Augen auch im Urteil **OGH 6 Ob 275/05t** vom 15. Dezember 2005 wieder.

³⁶⁴ Ein Testdatensatz wurde leider nicht zur Verfügung gestellt

³⁶⁵ LG Bonn vom 16.3.1993, CR 1995, 276 = WM 1994, 1285 = NJW-RR 1994, 1392

³⁶⁶ Schufa (D): Die **Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)** sammelt Daten über Verbraucher. Daten werden zB schon gespeichert, wenn ein Konto eröffnet wird. Bei denjenigen, die kein Konto haben, wird das in vielen Fällen an einer schlechten SCHUFA-Auskunft liegen.

Die SCHUFA selbst erhebt keine Daten, insbesondere führt sie keine Recherchen durch. (d.h. keine Auskünfte über gewerbliche Kunden sowie über Hypothekendarlehen) Sie ist eine reine Datensammelstelle und verlässt sich ganz und gar auf die Angaben ihrer Vertragspartner. Zusätzlich wertet Sie die Schuldnerverzeichnisse der deutschen Amtsgerichte aus, wie zB Abgabe der Eidesstattlichen Versicherung.

Vertragspartner der SCHUFA im europäischen Binnenmarkt sind beispielsweise Banken, Bausparkassen, Versicherungen, Versandhandelsunternehmen, Leasinggesellschaften, Kaufhäuser, Telekommunikationsunternehmen usw. Kreditvermittler sind nicht mehr Vertragspartner der SCHUFA.

Die Vertragspartner der SCHUFA erhalten von der SCHUFA zweierlei Arten von Auskünften: Die A-Auskunft und die B-Auskunft. B-Auskünfte enthalten nur Angaben darüber, ob sich ein Kunde vertragstreu verhalten und beispielsweise die Raten ordnungsgemäß zurückzahlt. Die A-Auskünfte sind schwerwiegender. Für Kreditvergabe, Führung eines Girokontos und die Ausgabe von Kreditkarten erhalten die Vertragspartner (in dieser Kategorie hauptsächlich Banken) neben den B-Auskünften Informationen über die gesamte Belastung; dazu ausführlich *Ganßauge*, Datenverarbeitung und –nutzung durch fremdnützige Verarbeiter, 30ff

Darin übernahm ein Wirtschaftsanwalt als Käufer einer Wohnung zur Besicherung eines vom Verkäufer aufgenommen Kredites die Haftung als Bürge und Zahler. Mit Wissen der Bank leistete er auch vereinbarungsgemäß Rückzahlungen. Als über das Vermögen des Verkäufers und Hauptschuldners der Privatkonkurs eröffnet wurde, stellte die Bank den Kredit fällig. Da die Bank und der Anwalt über den aushaftenden Betrag und die Rückzahlungsmodalitäten unterschiedlicher Auffassung waren, verweigerte der Anwalt vorerst die Tilgung. Daraufhin veranlasste die Bank seine Eintragung in die „Schwarze Liste“ ohne ihn darüber vorweg zu informieren. Dem Anwalt entgingen darauf hin zwei große Geschäfte und sein Ansehen wurde nachhaltig geschädigt und er wandte sich darauf hin an die Gerichte. Der OGH sowie auch die Vorinstanzen, qualifizierten die Eintragung als unverhältnismäßigen, rechtswidrigen Eingriff in die schutzwürdigen Interessen des Anwalts auf Geheimhaltung seiner Daten über die Kreditwürdigkeit. Diese Verletzung sei dazu geneigt, ihn in der Öffentlichkeit bloßzustellen³⁶⁷ und seine im Rahmen seines Berufes besondere Kreditwürdigkeit massiv zu beeinträchtigen. Zweck der Warnliste ist es, Auskunft über die Kreditwürdigkeit der Betroffenen zu erteilen. Sie sind somit als Daten iSd § 18 Abs 2 Z 3 DSG 2000 von der Anordnung des § 33 Abs 1 Satz 2 DSG 2000 umfasst. Die Eintragung in die Warnliste stellt eine öffentliche zugängliche Verwendung im Sinn dieser Bestimmung dar, und ist angesichts der großen Zahl an Teilnehmern an diesem Informationsverbundsystem nicht in Zweifel zu ziehen.

Die Bank hätte den Anwalt VOR der Fälligestellung des Kredits ausdrücklich darüber informieren müssen, dass wenn er nicht fristgerecht zahlt, in die Liste eingetragen werde. Dies sei sicherlich auf der einen Seite ein Druckmittel der Bank, zum anderen hätte der Jurist bei rechtzeitiger Information alles unternommen, um die Eintragung zu verhindern.

Die allgemein gehaltene „Datenschutzklausel“³⁶⁸ die bei Unterzeichnung des Kredits/Bürgschaft in den Verträgen enthalten ist, sei auf keinen Fall als ausreichende Warnung zu qualifizieren weil sie weder das Informationsmedium „Warnliste“ bezeichnet, noch einen konkreten Anlassfall anführt, der zur Eintragung in diese Liste führt, noch ausreichend konkret angibt, welche Daten für die Eintragung in die Liste verwendet

³⁶⁷ Siehe dazu *Dohr/Pollirer/Weiss*, Datenschutzrecht² § 33, 227

³⁶⁸ Diese lautete wie folgt: *Der Kreditnehmer erklärt sich einverstanden, „dass alle ihn betreffenden und im Rahmen dieses Kreditvertrages bekannt werdenden Daten in banküblicher Form, insbesondere im Interesse des Gläubigerschutzes oder zur Abwicklung von Bankgeschäften gemäß der ihm ausgehändigten Datenschutzerklärung, weitergegeben werden. Diese Ermächtigung erstreckt sich auch auf die Weitergabe von Daten aus diesem Kreditvertrag aus betrieblichen Gründen innerhalb der Bank und an Unternehmungen der Raiffeisen-Geldorganisation. Sie gilt auch als Ermächtigung für eine allgemein gehaltene Auskunft über die wirtschaftliche Lage“.*

werden.³⁶⁹ Zustimmung wird definiert als gültige Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt und diese liegt nur vor wenn der Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden.³⁷⁰ Es handelt sich hierbei um fehlende Informationen an den Betroffenen über die Übermittlung von Daten an einen Informationsverbund die aufgrund der Eingriffstiefe nach § 24 Abs 2 DSG 2000 notwendig gewesen wären und daher erfülle die „Datenschutzklausel“ die Voraussetzungen einer Zustimmung iSd § 3 Z 14 DSG 2000 nicht. Hier wird in die schutzwürdigen Interessen des Schuldners in unverhältnismäßiger Weise eingegriffen und liegt in einem solchen Fall ein Verstoß gegen den Grundsatz von Treu und Glauben vor da durch den Eintrag ein überwiegendes Gläubigerinteresse nicht mehr gerechtfertigt und daher rechtswidrig ist. Dies ist der Bank auch subjektiv vorwerfbar. Vor Weitergabe personenbezogener Daten an ein Kreditinformationssystem muss sich die Bank in jedem Fall vergewissern, ob eine schleppende Rückzahlung eines Kunden auf Zahlungsunfähigkeit oder Zahlungsunwilligkeit beruht andernfalls eine Meldung unzulässig ist.

Der OGH hat jedoch auch billigend festgestellt, dass aufgrund der Nichtzahlung bei Fälligkeit grundsätzlich der Anlass für die Aufnahme in die Warnliste gegeben war und der Verstoß des Beklagten gegen datenschutzrechtliche Bestimmungen darin bestand, dass dem Betroffenen/Kläger keine Möglichkeit geboten wurde, vor Aufnahme in die Warnliste Zahlungen zu leisten oder sich dagegen zur Wehr zu setzen. Die fehlende Aufklärung war auf jeden Fall kausal weil der Rechtsanwalt mit Sicherheit alles unternommen hätte um der Aufnahme in die „Warnliste“ zu entgehen, wenn er davon verständigt worden wäre da er nach Kenntniserlangung den Großteil der offenen Schuld auch sofort bezahlt hatte.

Neben dem Ersatz des Einkommensverlustes billigt der OGH auch den Zuspruch eines immateriellen Schadenersatzes da die Eintragung in die Warnliste zur verbreiteten Annahme verleitet, dass der Betroffene als Anwalt kreditunwürdig sei und dies „untergrabe sein Ansehen bei Klienten und unter Kollegen und ist geeignet, seinen Ruf nachhaltig zu schädigen und sogar seine wirtschaftliche Existenz zu gefährden“.³⁷¹ Der materielle Schaden ist jedoch ziffernmäßig iSd Bestimmtheitsgebots des § 226 ZPO aufzuschlüsseln,

³⁶⁹ Dies sollte mittlerweile durch die explizite Nennung der „Warnliste“ sowie der „KKE“ in den datenschutzrechtlichen Zustimmungserklärungen der Banken vermieden sein; so auch *Knyrim*, Die wichtigsten datenschutzrechtlichen Themen für Kreditinstitute, ÖBA 2007, 476 (488) der von einem „Rettungsanker“ spricht

³⁷⁰ Grundlegend OGH 22.3.2001 4 Ob 28/01y = SZ 74/52

³⁷¹ ÖBA 2006/1356 (OGH); Die Presse 20.2.2006

widrigenfalls die Klage unschlüssig sei.³⁷² Das unschlüssige Klagebegehren ist nicht nach hL und Rsp nicht sofort abzuweisen sondern dem Kläger ist eine Verbesserungsmöglichkeit einzuräumen.³⁷³ Die Höhe richtet sich nach dem Umfang und den Auswirkungen der Datenverwendung nach §§ 6 und 7 MedienG³⁷⁴, auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form einer Veröffentlichung in einem Medium geschieht.

10.5.2. Das Urteil OGH 1 Ob 38/88 vom 28.9.1988

Bereits im Jahr 1988 hat sich der OGH in seiner Entscheidung OGH 28.9.1988 **1 Ob 38/88** mit dem Eintrag in eine „vertrauliche Liste“ (=“Schwarze Liste“) befasst welche zu Unrecht erfolgt ist und hat festgestellt, dass nur aus der Tatsache der Einleitung der Fahnisexekution, ohne jede weitere Erhebungen durchzuführen ob tatsächlich Zahlungsschwierigkeiten vorliegen, auf einem Sorgfaltsverstoß iSd § 1330 ABGB³⁷⁵ beruht. Zum damaligen Zeitpunkt wurden diese Informationen noch schriftlich in regelmäßigen Druckwerken an die Mitglieder des Gläubigerschutzverbandes ausgesandt.

Der Gläubiger konnte aufgrund des Wohnungskaufs und der damit verbundenen Renovierung erkennen, dass der Betroffene noch an einer anderen Anschrift wohnt, Angestellter ist gegen den Gehaltsexekution geführt werden könnte und lediglich einen Teil der offenen Rechnung aufgrund einer Reklamation nicht sofort beglich. Zur Haftung des Verbreiters nach § 1330 Abs 2 erster und zweiter Satz ABGB genügt nach herrschender Rechtsauffassung jede, also auch leichte Fahrlässigkeit.³⁷⁶ Auch der Einwand die Mitteilung erstreckt sich nur an einen vorausbestimmten Empfängerkreis und ist vertraulich hat der OGH bereits in der E EvBl 1988/32 festgestellt, dass dann, wenn das Gebot der Vertraulichkeit auch nur einer Person gegenüber nicht gewahrt wird, der Mitteilende sich nicht auf die Nichtöffentlichkeit der Mitteilung berufen dürfe. Die herrschende Auffassung ist dahin zu interpretieren, dass die Voraussetzungen für die Nichtöffentlichkeit einer Mitteilung eher streng beurteilt werden. Eine solche Gewähr der Nichtöffentlichkeit ist auszuschließen, wenn ein großer

³⁷² ZIK 2006/82, 68; OGH 13.7.2000 6 Ob 30/00f; OGH 6.10.2005 6 Ob 51/05a

³⁷³ RIS-Justiz RS 0036355

³⁷⁴ Berka/Höhne/Noll/Polley, Mediengesetz², Rz 43 f

³⁷⁵ § 1330 lautet: (1) Wenn jemandem durch Ehrenbeleidigung ein wirklicher Schade oder Entgang des Gewinnes verursacht worden ist, so ist er berechtigt, den Ersatz zu fordern.

(2) Dies gilt auch, wenn jemand Tatsachen verbreitet, die den Kredit, den Erwerb oder das Fortkommen eines anderen gefährden und deren Unwahrheit er kannte oder kennen mußte. In diesem Falle kann auch der Widerruf und die Veröffentlichung desselben verlangt werden. Für eine nicht öffentlich vorgebrachte Mitteilung, deren Unwahrheit der Mitteilende nicht kennt, haftet er nicht, wenn er oder der Empfänger der Mitteilung an ihr ein berechtigtes Interesse hatte.

³⁷⁶ JBl 1987, 724; ÖBl 1979, 134; RZ 1979/69; EvBl 1978/99 ua); Harrer aaO Rz 25; Reischauer in Rummel, ABGB, Rz 16 zu § 1330; Koziol aaO 176 f

Gläubigerschutzverband ein Mitteilungsblatt in großer Auflage an alle seine Mitglieder hinaus gibt und nach dem Inhalt der Mitteilungen nicht ernstlich annehmen kann, dass ihre Kenntnis auf den Kreis der Mitteilungsempfänger beschränkt bleibt. Der ausdrückliche Hinweis auf die Vertraulichkeit der Mitteilungen muss inhaltsleer bleiben, wenn alle Beteiligten und insbesondere die beklagte Partei wissen müssen, dass sie nicht gewahrt werden kann. Schon nach dem Wesen und schon gar nach der sinnvollen Anwendung der nicht zu Unrecht so bezeichneten "Schwarzen Liste" ist es gerade zu unvermeidbar, dass auch zahlreiche Personen, die nicht Empfänger der Liste sind, ihren Inhalt erfahren. So war es sicher nicht nur ein normalerweise auszuschließender Zufall, dass auch der Dienstgeber des Klägers, weil er der beklagten Partei angehört, und dessen Kollegen von der Aufnahme des Klägers in die Liste erfuhren. Gerade bei Personen, deren Aufnahme in die Liste man nicht erwartet, spricht sich solches als Sensation rasch herum. Dass die beklagte Partei selbst ihre Mitteilungen nicht als nichtöffentlich ansieht, ergibt sich daraus, dass sie diese Informationen/Mitteilungen in ihren Hinweisen an die Bezieher selbst als "Veröffentlichungen" bezeichnet.

Warum auf dieses Urteil in der Entscheidung 6 Ob 275/05t vom 15. Dezember 2005 (siehe oben Kapitel 10.5.1.) und auch in den Vorinstanzen nicht Bezug genommen wurde, entzieht sich meiner Kenntnis obwohl der Sachverhalt ähnlich gelagert ist. Es hat sich zwar die Form der Datenübertragung/Informationstechnik in den letzten 17 Jahren geändert aber der Grundgehalt des Sorgfaltsmaßstabes sowie ein ähnlich gelagerter Sachverhalt hätte schon vorher eine klare rechtliche Stellungnahme offeriert.

10.5.3. Das Urteil LG ZRS Wien 9 Cg 216/99x vom 21.2.2000

Ein weiteres interessantes Urteil stammt bereits aus dem Jahr 2000 und dürfte mittlerweile auch in die Arbeits- und Vorgangsweise der beteiligten Banken Einzug gehalten haben. Normalerweise bzw. bis zu dem Urteil **9 Cg 216/99x** des LG für ZRS Wien vom 21.2.2000 wurde zB eine „dritte Mahnung“ bis zu 5 Jahre, die Meldung einer Klage oder Exekution bis zu 10 Jahre lang nach Bezahlung die betroffene Person in der an- bzw. weitergeführt Diese Meldungen seien unabhängig von der Höhe der Forderung obwohl diese dem KSV mitgeteilt wird. Sinn einer solchen UKV Negativmeldung sei es, dass der Kunde bei einer Vorsprache bei einem anderen Kreditinstitut etwas zur Errichtung eines Kontos oder zur Aufnahme eines Kredits genauer geprüft werde und die andere Bank bei Einräumung eines Kredits auf verstärkte Sicherheiten achte. Eine solche Negativmeldung sei jedoch in keinem Fall derart

verbindlich, dass eine andere Bank die Errichtung eines Kontos oder die Einräumung eines Kredits überhaupt verweigern müsse.

In diesem Fall hatte Herr B. sein Girokonto überzogen, Teilzahlungen geleistet und den Gesamtbetrag nach Klage inklusive Anwaltskosten beglichen. Einer Aufforderung von Herrn B. zur Löschung dieses Eintrages verweigerte die Bank worauf sich dieser an das Gericht wandte. Das LGZ gab ihm Recht, da Herr B. ja „auf die Mahnung reagiert und nach der Klage auch alles bezahlt habe“. Da es sich dabei auf um vergleichsweise geringe Summen handelte und mittlerweile auch schon einige Zeit vergangen ist, ist das Interesse des Kunden an einer Löschung höher zu bewerten als das Interesse der Banken, schwarze Schafe an den Pranger zu stellen.

Die Hauptgründe für die Fehlerhäufigkeit von Bonitätsauskünften dürfte sich in der relativ großen Anzahl unter Zeit- und Kostendruck erstellten Auskünfte, mangelnden Qualifikation von Rechercheuren, unsystematische Auswertung von Informationsquellen, mangelnde Aktualität, mögliche Interessenskonflikte der Informationsgeber und häufig allzu pauschale Abfassung der Auskünfte zu finden sein.³⁷⁷

10.5.4. Rechtliche Beurteilung

Die „Negativliste der Banken“ (auch UKV bzw „Schwarze Liste“) unterliegt der Vorabkontrolle iSd § 18 Abs 2 Z 3 DSG 2000 da sie die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Inhalt hat und darüber hinaus in Form eines Informationsverbundsystems geführt wird (§ 18 Abs 2 Z 4 DSG 2000). Gemäß § 50 DSG 2000 ist für ein Informationssystem die Bestellung eines Betreibers (in diesem Fall der KSV) notwendig wobei Name und Anschrift in der Meldung zur Eintragung in das DVR bekannt zugeben sind. Der Kreditschutzverband ist daher auch erster Ansprechpartner des Betroffenen, falls diesem der konkrete Auftraggeber nicht bekannt ist und hat innerhalb von zwölf Wochen diesem alle Auskünfte zu geben (§ 50 Abs 1 DSG 2000), die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen. Ferner ist er auch für die Datensicherheitsmaßnahmen iSd § 14 DSG 2000 im System verantwortlich.³⁷⁸

³⁷⁷ Peilert, Das Recht des Auskunft- und Detektengewerbes, 127 ff

³⁷⁸ Jähnel, Das Datenschutzgesetz 2000, Wichtige Neuerungen, wbl 02/2000, 55

Wie bereits oben erwähnt, würde die Meldung an eine Evidenzstelle, dass Kreditverpflichtungen nicht nachgekommen wird oder Bankomat- und/oder Kreditkarten missbräuchlich verwendet werden ohne Vorliegen einer Zustimmungserklärung einen Verstoß gegen das Bankgeheimnis iSd § 38 BWG bedeuten. Diese Zustimmungserklärung bedeutet sodann gleichzeitig die Zulässigkeit nach §§ 1 und 7, 8 DSG 2000.

*Weissel*³⁷⁹ stimmt dem insoweit zu als auch ein rechtswidrig agierender Kunde seinen Geheimhaltungsanspruch nicht verliert was § 23 Abs 1 Z 5 KWG (nunmehr § 38 Abs 2 Z 7 BWG) zeigt, der die Bank zur Offenbarung von Kundengeheimnissen ermächtigt sofern dies zur Klärung von Rechtsangelegenheiten zwischen Kunden und Kreditinstitut notwendig ist.

Der Umkehrschluss daraus, wonach die Bank in diesen Fällen Dritten gegenüber zur Verschwiegenheit verpflichtet ist, lässt sich daraus in seinen Augen jedoch nicht schließen, da § 23 Abs 2 KWG (nunmehr § 38 Abs 2 BWG) keine abschließende Aufzählung jener Fälle enthält, in welchen die Verschwiegenheitspflicht der Bank entfällt.

Würde sodann ein betroffener Kunde seine Zustimmungserklärung widerrufen, so ist diese jedoch zu beachten. Eine Datenweitergabe darf jedoch dennoch erfolgen, da anstatt der Zustimmung iSd § 8 Abs 1 Z 2 DSG 2000 der Grund der überwiegenden berechtigten Interessen des Auftraggebers iSd § 8 Abs 1 Z 4 DSG 2000 tritt und das Interesse des Kreditinstituts weitaus höher zu bewerten ist als jenes der Weitergabe der Informationen des Betroffenen. Gleichzeitig ist jedoch unter der Prämisse des Gläubigerschutzes eine Übermittlung nur gerechtfertigt, wenn die die betreffenden Daten zuverlässig und objektivierte Aussagen über die mangelnde Kreditfähigkeit oder –würdigkeit des Betroffenen beinhalten.³⁸⁰ Dieses Prinzip lässt sich insbesondere aus der ergangenen OGH Entscheidung³⁸¹ zu § 1330 ABGB ableiten wo einem Gläubigerschutzverband keine Fahrlässigkeit vorgeworfen werden kann wenn er den Namen eines Schuldners in seinen Aussendungen nennt gegen den Fahrnisexekution geführt wird. Wobei idR davon ausgegangen werden kann, dass Exekutionen Zahlungsunfähigkeit indizieren.³⁸²

Unstrittig sind danach jedenfalls jene Fälle, wo das angestrengte Exekutionsverfahren nicht zur Hereinbringung der Forderung geführt hat oder ein Insolvenzverfahren zwischenzeitlich eröffnet wurde bzw mangels Masse abgewiesen wurde.

Liegt diesbezüglich keine titulierte Forderung vor, so kommt es auf die Umstände des Einzelfalles an, wobei zugunsten des Betroffenen festgehalten werden muss, dass eine

³⁷⁹ *Weissel*, Das Bankgeheimnis in der österreichischen Grundrechtsordnung, ÖZW 1989, 80ff (81ff)

³⁸⁰ *Stadler*, Wirtschaftsinformationen und Datenschutz, 12; *Feuerborn* in *Sichtermann-Feuerborn-Kirchherr-Terdenge*, Bankgeheimnis und Bankauskunft, 444

³⁸¹ OGH 20.10.1987 4 Ob 338/87, wbl 1988, 99ff

³⁸² OGH 08.05.1984 4 Ob 559/83 = SZ 57/87 = EvBl 1985/92, 461 = JB1 1985,494 = RdW 1984,242

objektive Verifizierung über die Richtigkeit des geltend gemachten Anspruchs fehlt und der Empfänger der (Negativ-)Information keine Klarheit darüber hat ob nicht berechnigte Einwendungen dagegen erhoben wurden.

Ein Verstoß gegen § 38 BWG (Bankgeheimnis) liegt nach hL und Rsp nicht vor, da die Ausnahmetatbestände darin als nicht taxativ angesehen werden und es auch andere Ausnahmetatbestände gibt. (zB Meldung an die Großkreditevidenz iSd § 75 BWG, Aufklärungspflichten von zukünftigen Bürgen bzw Diskontnehmern iSd § 25c KschG³⁸³)

Nachdem das BWG und die darin befindlichen Schutzbestimmungen prinzipiell die Funktionsfähigkeit des Banken- und Kreditapparates sicherstellen sollen, kann nicht angenommen werden, dass den Banken, anders als dem durch den Gesetzgeber als weniger schutzwürdig anerkanntensontigen Unternehmen, die (Ein-)Führung ein solches Schutzinstrument verwehrt wird.³⁸⁴

Das Gläubigerschutzinteresse wird in einem solchen Falle auf jeden Fall höher einzustufen sein als das Geheimhaltungsinteresse des Betroffenen. Desweiteren bleibt der Adressatenkreis beschränkt und geschlossen und ist für Außenstehende nicht einsehbar.

Die Bankgeheimnisbestimmungen stehen daher einer Meldung nicht entgegen, da zwar die einmal gegebene Zustimmungserklärung ausreichend und der Widerruf iSd § 8 Abs 1 Z 2 DSG 2000 beachtlich ist aber anstatt dieses Übermittlungsgrundes nun § 8 Abs 1 Z 4 DSG 2000 („überwiegend berechnigte Interessen des Auftraggebers oder eines Dritten“) zu Tage tritt. Bei Vorliegen überwiegender berechnigter Interessen Dritter ist daher auch keine Verletzung schutzwürdiger Interesses des Täters/Betroffenen zu sehen.³⁸⁵

Anlässlich der Registrierung der UKV-Warnliste wurde jedem teilnehmenden Auftraggeber die Auflagen gemäß § 21 Abs 2 DSG 2000 für die Vornahme der Datenanwendung durch Bescheid von Seiten der DSK erteilt.³⁸⁶ Der OGH geht in seiner E bezüglich Warnlisten von nicht kreditwürdig eingestuften Kunden unter dem Aspekt des berechnigten Interesses des Gläubigerschutzes, prinzipiell von einer Zulässigkeit aus.³⁸⁷

10.6. Die WKE – WarenKreditEvidenz - Datenbank

³⁸³ RdW 1988, 130; OGH 7.9.1989 8 Ob 629/89, ecolex 1990, 18; OGH 9.2.1988 6 Ob 508,509/86; SZ 58/153

³⁸⁴ *Weissel*, Die Negativliste der Banken aus datenschutzrechtlicher Sicht, EDVuR 1990, 62

³⁸⁵ So schon *Potyka*, Datenschutz in der Wirtschaft, 138ff zu § 18 DSG 1978; *Pruckner*, Datenschutz im Kreditwesen 147

³⁸⁶ GZ K095.014/016-DSK 2001 und GZ K095.014/021-DSK 2001 vom 23. November 2001

³⁸⁷ OGH 15.12.2005 6 Ob 275/05t = ÖJZ 2006/66 = ecolex 2006/211 = MR 2006, 83

Die WKE ist lt. Eigendefinition des KSV die bedeutendste Negativdatenbank da mit Anbindung an diesen Datenpool sehr viele warenkreditgebende Unternehmen der Wirtschaft ihrer Forderungsausfälle im Privatkundensegment verringern können. Eine, wenn auch relativ lange Liste aller Teilnehmer, wurde nicht bekannt gegeben.

Die Umfang der Datenbank ist wie folgt: (Stichtag 31.12.2007)

	2007	2006	2003
Personen mit Negativa	376.495	189.264	ca. 365.000
Zahlungsanstände	518.184	531.259	566.981
Jährliche Anfragen beim KSV	393.348	830.000	ca. 1.100.000
Selbstauskünfte	31.418	25.090	16.487
Teilnehmer/Einmelder	393	291	423

Der KSV hat im Jahr 1997 die WKE in Zusammenarbeit mit den größten Versandhäusern Österreichs gegründet. Zweck ist es Negativerfahrungen mit einzelnen Kunden zu teilen wo auf offene Rechnung geliefert wird. Zugang zur WKE hat nur ein eingeschränkter, vertraglich verpflichteter Teilnehmerkreis da die Berechtigung zur Abfrage auch die Pflicht zur Einmeldung voraussetzt. Dh nur wer einmeldet, darf auch abfragen. Teilnehmer sind ua Versandhäuser, Telekommunikations- und Einzelhandels-unternehmen, Lagerhäuser, Banken, Leasingunternehmen, uvm. Jedoch steht für die Unternehmen der Telekommunikationsindustrie § 96 TKG entgegen welches jegliche Weitermeldung von Teilnehmerdaten verbietet wodurch das Prinzip der Reziprozität zumindestens in diesem Industriezweig als aufgehoben angesehen werden kann. Andererseits sieht das TKG in § 92 Abs 3 Z 3 lit f iVm § 97 Abs 1 die Verarbeitung von Bonitätsdaten durch Betreiber ausdrücklich vor. Die Überprüfung der Kundenbonität kann als überwiegendes Interesse im Sinne des § 1 Abs 2 DSG 2000 angesehen werden. Für Aktualität und Richtigkeit sorgen die laufenden Einmeldungen der registrierten Teilnehmer. Diesen Daten werden mit aktuellen Inkasso- und Insolvenzinformationen verknüpft. Abhängig von der Eskalationsstufe enthält jeder Eintrag eine Löschfrist. Ist sie abgelaufen, werden die Daten automatisch gelöscht.

Im unten angeführten Beispiel wird die Funktionalität der Datenbank kurz gezeigt.

Nach Eingabe der Benutzerkennung und Passwort kann eine Abfrage gestartet werden.

KSV1870

my KSV | [Produkte](#) | [News](#) | [Der KSV](#) | [Mitgliedschaft](#)

[Auskünfte](#) | [Monitoring](#) | [Inkasso](#) | [Insolvenz](#) | [Weitere Services](#) | [Privatinformation](#)

[Preise](#) | [Meine Einstellungen](#)

KSV >> My KSV

My Login

User:

Password:

Identification:

[Login >>](#)

[Noch nicht angemeldet?](#) [Jetzt registrieren!](#)

Abfrage nach Personendaten

Benutzername: KERNMAYERD01

Alle Felder mit ■ sind Pflichtfelder und müssen ausgefüllt werden!

Suche nach:

■ Titel, Vorname		
■ Nachname		
■ PLZ/Ort		
■ Straße, Hausnummer		

☐ genaue Suche ☒ phonetische Suche

€ Kostenpflichtig: [Suchen >>](#)

Allererst erfolgt eine Adressverifizierung – dh ob es den Kunden tatsächlich gibt und wo er wohnt. Dies allein soll eine Verringerung des Delekrederisikos um 60 % bringen.

Ihre Suche lautete:

Vorname: franz
Nachname: test
Geburtsdatum: 01.01.1900

Ergebnis WKE

1

[Alle anzeigen](#)

[Geschäftsfälle anzeigen](#)

Auftragsnummer	Titel	Vorname	Nachname	Geboren	Adresse	PLZ	Ort
19185050		FRANZ	TEST	01.01.1900	TESTSTRASSE 1	1110	WIEN

1

[Alle anzeigen](#)

[Geschäftsfälle anzeigen](#)

Ergebnis Adressprüfung

Die Adressprüfung ergab keinen Treffer

[AGB](#) | [Impressum](#) | [Downloads](#) |

Danach werden die Daten mit der WKE Datenbank abgeglichen:

Person abfragen: Ergebnis Geschäftsfälle

Vorname: FRANZ
Nachname: TEST
Adresse: TESTSTRASSE 1, -1110 WIEN
Geboren: 01.01.1900
Auftragsnummer 19185050

Anzahl der Einmelder: 1

Datum des Anstandes	Anstandscode	Anstandscode	Betrag	Währung
28.07.2008	0110	RATENZAHUNG VEREINBART NACH INKASSOBÜRO		500EUR

Zurück

Drucken

Historie anzeigen

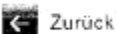
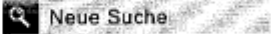
Neue Suche

[AGB](#) | [Impressum](#) | [Downloads](#) |

In einer „Tiefensuche“ (Historie) kann der Geschäftsfall von Beginn bis zum aktuellen status quo nach verfolgt werden:

Person abfragen: Historie zum ausgewählten Geschäftsfall

Datum des Anstandes	Anstandscode	Anstandscode Text	Betrag	Währung
28.07.2008	0110	RATENZAHLUNG VEREINBART NACH INKASSOBÜRO		500EUR
27.07.2008	0100	ÜBERGABE INKASSOBÜRO		900EUR

[AGB](#) | [Impressum](#) | [Downloads](#) |

Um eine Person eindeutig identifizieren zu können ist idR das Geburtsdatum unerlässlich. Ein leicht geändertes Geburtsdatum (von 1.1.1900 auf 02.01.1900) bringt kein Ergebnis/Treffer.

Ihre Suche lautete:

Vorname: franz
Nachname: test
Geburtsdatum: 02.01.1900

Ergebnis WKE

Keine Negativeinträge vorhanden.



Ergebnis Adressprüfung

Die Adressprüfung ergab keinen Treffer

[AGB](#) | [Impressum](#) | [Downloads](#) |

Aufgrund der bedingten Gegenseitigkeit von Abfragemöglichkeit und Einmeldepflicht gibt es auch die direkte Einmeldemöglichkeit von Personen mit Negativmerkmalen:

Neueinmeldung einer Person

Benutzername: KERNMAYERD01

Alle Felder mit * sind Pflichtfelder und müssen ausgefüllt werden! * bezeichnet optionale Felder entweder

Person	
* Anrede	
* Titel, Vorname	
* Nachname	
* Geburtsdatum	. . jiji.mm.tt
* PLZ/Ort	/
* Straße, Hausnummer, Stiege/Stock/Tür	
Landeskennzahl	Österreich
Geschäftsfall	
* Kundennummer:	
* Geschäftsfall-Nummer:	
* Zahlungsanstand Code:	Bitte wählen Sie aus ...
* Datum des Anstandes:	. . jiji.mm.tt
* Betrag:	EUR
Einmelden	

Code		BETREIBUNGSART	MELDUNGSART	LÖSCHFRISTEN	KORREKTURLAUF
0000		Übergabe außergerichtliche Betreuung	Eskalatio	b.a.w.	6 Monate
0010		Ratenzahlung vereinbart nach außergerichtlicher Betreuung	Positivmeldung	b.a.w.	12 Monate
0020		Teilzahlung nach außergerichtlicher Betreuung	Positivmeldung	b.a.w.	12 Monate
0030		Beahlt nach Vergleich	Positivmeldung	5 Jahre	
0050	X	Beahlt nach außergerichtlicher Betreuung	Positivmeldung	5 Jahre	
0060		Forderung zurückgewiesen (Anspruch ungeklärt)	Information	5 Jahre	
0070		Forderung aus wirtschaftlichen Gründen ausgebucht	Eskalation	10 Jahre	
0090		Storno	Information	1 Monat	
0100		Übergabe Inkassobüro	Eskalation	b.a.w.	6 Monate
0110		Ratenzahlung vereinbart nach Inkassobüro	Positivmeldung	b.a.w.	12 Monate
0120		Teilzahlung nach Inkassobüro	Positivmeldung	b.a.w.	12 Monate
0130		Beahlt nach Vergleich	Positivmeldung	10 Jahre	
0150	X	Beahlt nach Inkassobüro	Positivmeldung	5 Jahre	
0160		Inkassobüro bestritten	Information	5 Jahre	
0170		Uneinbringlichkeit nach Inkassobüro	Eskalation	10 Jahre	
0180		Erledigung unklar	Information	10 Jahre	
0190		Storno nach Inkassobüro	Information	1 Monate	
0200		Übergabe Rechtsanwalt	Eskalation	b.a.w.	6 Monate

0210		Ratenzahlung vereinbar mit Rechtsanwalt	Positivmeldung	b.a.w.	12 Monate
0220		Teilzahlung nach Rechtsanwalt	Positivmeldung	b.a.w.	12 Monate
0250	X	Bezahlt nach Rechtsanwalt	Positivmeldung	5 Jahre	
0260		Rechtsanwalt bestritten	Information	5 Jahre	
0270		Uneinbringlichkeit nach Rechtsanwalt	Eskalation	10 Jahre	
0290		Storno nach Rechtsanwalt	Information	1 Monate	
0300		Übergabe gerichtliche Betreuung	Eskalation	b.a.w.	12 Monate
0310		Ratenzahlung vereinbart nach gerichtlicher Betreuung	Positivmeldung	b.a.w.	12 Monate
0320		Teilzahlung nach gerichtlicher Betreuung	Positivmeldung	b.a.w.	12 Monate
0330		Bezahlt nach Vergleich	Positivmeldung	10 Jahre	
0350	X	Bezahlt nach gerichtlicher Betreuung	Positivmeldung	10 Jahre	
0360		Gerichtliche Betreuung bestritten	Information	5 Jahre	
0370		Uneinbringlichkeit n. gerichtlicher Betreuung	Eskalation	10 Jahre	
0375		Uneinbringlichkeit nach Zustellanstand	Eskalation	10 Jahre	
0390		Storno nach gerichtlicher Betreuung	Information	1 Monate	
0400		Klage eingereicht	Eskalation	b.a.w.	12 Monate
0410		Ratenzahlung vereinbart nach Klage	Positivmeldung	b.a.w.	12 Monate
0420		Teilzahlung nach Klage	Positivmeldung	b.a.w.	12 Monate
0450	X	Bezahlt nach Klage	Positivmeldung	10 Jahre	
0460		Klage bestritten	Information	5 Jahre	
0470		Uneinbringlichkeit nach Klage	Eskalation	10 Jahre	
0490		Storno nach Klage	Information	1 Monat	
0500		Exekution eingeleitet	Eskalation	b.a.w.	12 Monate
0510		Ratenzahlung vereinbart nach Exekution	Positivmeldung	b.a.w.	12 Monate
0520		Teilzahlung nach Exekution	Positivmeldung	b.a.w.	12 Monate
0550	X	Bezahlt nach Exekution	Positivmeldung	10 Jahre	
0560		Exekution bestritten	Information	5 Jahre	
0570		Uneinbringlichkeit nach Exekution	Eskalation	30 Jahre	
0590		Storno nach Exekution	Information	1 Monate	
0700		Zum Insolvenzverfahren abgetreten	Information	10 Jahre	
0999		Eigensperre	Information	b.a.w.	
0998		Widerruf	Information	b.a.w.	
7001		Insolvenz kann nicht ausgeschlossen werden	KSV		12 Monate
7110		Außergerichtliches Sanierungsverfahren eingeleitet	Insolvenzmeldung		12 Monate
7180	X	Außergerichtliches Sanierungsverfahren wurde direkt abgewickelt	Insolvenzmeldung	7 Jahre	
7190	X	Außergerichtliche Sanierung ist gescheitert	KSV	7 Jahre	
7200	X	Außergerichtliche Entschuldung mit allen Gläubigern	Positivmeldung	5 Jahre	
7203		Vorverfahren wurde beantragt	KSV		12 Monate
7210		Vorverfahren wurde eröffnet	KSV		12 Monate

7280	X	Verpflichtungen aus Vorverfahren direkt abgewickelt	KSV	7 Jahre	
7284	X	Verpflichtungen aus Vorverfahren erfüllt	KSV	5 Jahre	
7289		Verpflichtungen aus Vorverfahren wurde nicht erfüllt	KSV	7 Jahre	
7303		Ausgleich wurde beantragt	KSV		12 Monate
7310		Ausgleich wurde eröffnet	KSV		12 Monate
7311		Ausgleichseröffnung durch Überleitung eines Vorverfahrens	KSV		12 Monate
7374		Ausgleich wurde gerichtlich bestätigt	KSV		12 Monate
7377		Ausgleich wurde gerichtliche Bestätigung versagt – Anschlusskonkurs wird erwartet	KSV		12 Monate
7380	X	Ausgleich wurde direkt abgewickelt	KSV	7 Jahre	
7382		Ausgleichsverfahren wurde aufgehoben und befindet sich im Erfüllungsstadium	KSV		12 Monate
7384	X	Ausgleich wurde erfüllt	KSV	5 Jahre	
7390		Ausgleichsverfahren wurde eingestellt – über eine Anschlusskonkursöffnung wird vom Gericht entschieden	KSV		12 Monate
7391		Ausgleichsverfahren wurde eingestellt – Anschlusskonkurs ist mangels Kostendeckung nicht erfolgt	KSV		12 Monate
7403		Konkurs wurde vom Schuldner beantragt	KSV		12 Monate
7410		Konkurs wurde eröffnet	KSV		12 Monate
7462		Zahlungsplan wurde beantragt *)	KSV		12 Monate
7472		Zahlungsplan von Gläubigern angenommen *)	KSV		12 Monate
7474		Zwangsausgleich/ZP gerichtlich bestätigt	KSV		12 Monate
7480	X	Zwangsausgleich/ZP wurde vom Schuldner direkt abgewickelt	KSV	7 Jahre	
7481		Konkursaufhebung nach Abschluss eines Zwangsausgleiches/Zahlungsplanes	KSV		12 Monate
7482	X	Zahlungsplan wurde direkt abgewickelt *)	KSV	7 Jahre	
7483		Konkursaufhebung nach rechtskräftiger Einleitung eins Abschöpfungsverfahrens	KSV		12 Monate
7484	X	Zwangsausgleich/Zahlungsplan wurde erfüllt	KSV	5 Jahre	
7485	X	Zahlungsplan wurde erfüllt *)	KSV	5 Jahre	
7490		Zwangsausgleich/ZP wurde nicht erfüllt	KSV	7 Jahre	
7492	X	Konkursaufhebung nach Rekurs gegen den Eröffnungsbeschluss	KSV	3 Jahre	
7500	X	Konkursaufhebung	KSV	10 Jahre	
7510		Konkurs wurde eröffnet *)	KSV		12 Monate
7563		Abschöpfungsverfahren eingeleitet *)	KSV		12 Monate
7574		Zwangsausgleich/ZPlan gerichtlich bestätigt und befindet sich im Erfüllungsstadium *)	KSV		12 Monate
7575		Zahlungsplan gerichtlich bestätigt *)	KSV		12 Monate
7581		Konkursaufhebung nach Abschluss eines Zwangsausgleiches/Zahlungsplans *)	KSV		12 Monate

7582		Konkursaufhebung nach Abschluss *)	KSV		12 Monate
7583		Konkursaufhebung nach rechtskräftiger Einleitung eines Abschöpfungsverfahrens *)	KSV		12 Monate
7585	X	Abschöpfungsverfahren vorzeitig eingestellt ohne Restschuldbefreiung *)	KSV	10 Jahre	
7586	X	Restschuldbefreiung erwirkt *)	KSV	5 Jahre	
7589	X	Widerruf der Restschuldbefreiung	KSV	5 Jahre	
7592		Konkursaufhebung nach Rekurs gegen den Eröffnungsbeschluss	KSV	3 Jahre	
7600	X	Konkursaufhebung *)	KSV	10 Jahre	
7900	X	Abweisung eines Konkursantrages mangels Kostendeckung	KSV	10 Jahre	
0600		Übernahme Dubioseninkasso	Eskalation	30 Jahre	
0620		Dubioseninkasso Teilzahlung	Positivmeldung	30 Jahre	
0630	X	Dubioseninkasso bezahlt nach Vergleich	Positivmeldung	30 Jahre	
0640		Dubioseninkasso – Adresse wird abgeklärt	Information	30 Jahre	
0650	X	Dubioseninkasso –Forderung bezahlt	Positivmeldung	5 Jahre	
0670		Dubioseninkasso – Forderung uneinbringlich	Eskalation	30 Jahre	
0680		Dubioseninkasso– Uneinbringlich n. Teilzahlung	Eskalation	30 Jahre	
0690		Dubioseninkasso – Storno	Information	1 Monat	

Legende: b.a.w. = Dauer ist abhängig von der Statusmeldung; X=Forderung erledigt; *) Privatsolvenzverfahren

10.6.1. Rechtliche Beurteilung

Die Warenkreditevidenz Datenbank (WKE) unterliegt der Vorabkontrolle iSd § 18 Abs 2 Z 3 DSG 2000 da sie die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Inhalt hat und darüber hinaus in Form eines Informationsverbundsystems geführt wird (§§ 18 Abs 2 Z 4 bzw § 50 DSG 2000). Dies wurde auch von der DSK bestätigt.

Die darin eingemeldeten und weitergegebenen Daten unterliegen den schutzwürdigen Geheimhaltungsinteressen nach § 1 DSG 2000. Die Dateneinmeldung wird durch die ausdrückliche Zustimmung bei Vertragsabschluß des Kunden mit dem jeweiligen Lieferanten iSd § 8 Abs 1 Z 2 DSG 2000 legitimiert.

Die Datenverwendung iSd § 7 DSG 2000 ist durch § 152 GewO rechtlich gedeckt.

Die Übermittlung iSd § 7 Abs 2 DSG 2000 erfolgt aufgrund § 8 Abs 1 Z 4 DSG 2000 („überwiegend berechnigte Interessen des Auftraggebers oder eines Dritten“).³⁸⁸

Ob es sich hiebei um eine „öffentlich zugängliche Datenbank“ handelt oder nicht ist zwischen Lehre und Judikatur strittig. Aufgrund des bestehenden geschlossenen Benutzerkreises ist in meinen Augen von einer „nicht öffentlich zugänglichen“ Datenbank auszugehen.³⁸⁹ Das Kriterium der Entgeltlichkeit ist kein Argument welches zur Lösung der Definition beitragen kann.³⁹⁰ Näheres hiezu siehe Kapitel 11.1.

³⁸⁸ So urteilt der BGH „So werden die berechtigten Interessen der Allgemeinheit an einem Schutz vor der Vergabe von Krediten an Zahlungsunfähige oder –unwillige eine Weitergabe von Daten über die Eröffnung des Konkursverfahrens, die eidesstattliche Versicherung (...) durch den Schuldner oder die Zwangsvollstreckung in sein Vermögen in aller Regel rechtfertigen“, NJW 1984,436 [437]

³⁸⁹ Zustimmend Koch, Informations-, Aufklärungs- und Sorgfaltspflichten bei der Kreditvergabe nach der neuen RL 2008/48/EG vom 23.4.2008 über Verbraucherkreditverträge, ÖBA 2009, 98

³⁹⁰ Ausführlich Forgo, Das Widerspruchsrecht nach § 28 Abs 2 DSG 2000, JusIT 1/2009, 18ff

11. Deltavista GmbH Österreich

Unternehmenshistorie

Vorher	...gab es keine effiziente Lösung, um bestehende und neue Kundendaten mit Zahlungserfahrungen und Adressdetails zu aktualisieren, zu ergänzen und zu vervollständigen.
1994	Deltavista wird gegründet, um diese Marktlücke zu schließen. Damals firmierte Deltavista unter dem Namen IQA.
1996	Es wird offensichtlich, dass die im Markt erhältliche Software nicht ausreicht, um eine effiziente Plattform für den Austausch von adressbezogenen Daten zu bauen. Daher beginnt Deltavista, die Lücken mit eigenen Softwareentwicklungen zu schließen und ein Team an hervorragenden Software-Ingenieuren aufzubauen.
1998	Die Plattform OK-online mit dem Fokus auf Risikomanagement wird produktiv gesetzt. Deltavista gewinnt den ersten großen Mobilfunk Provider, sowohl für Firmen- als auch für Privatpersonprüfungen
2000	<u>Gründung der österreichischen Niederlassung in Wien.</u> Deltavista wächst auf 16 Mitarbeiter.
2001	Gründung der polnischen Niederlassung in Krakau. Gründung der deutschen Niederlassung in München. Der Firmenname wird von IQA auf Deltavista geändert. Deltavista wächst auf 32 Mitarbeiter.
2002	Deltavista wächst auf 85 Mitarbeiter, davon sind 65 qualifizierte Software-Ingenieure.
2003	OK-online wird in Deltavista Online umbenannt und die Funktionalitäten, das Design und die Benutzerfreundlichkeit stark verbessert. Deltavista wächst auf über 110 Mitarbeiter, davon sind 85 hoch qualifizierte Software-Ingenieure.
2004	Nachdem die Aktionärsstruktur bereinigt wird, fokussiert Deltavista seine Strategie auf Daten – Daten – Daten: „Deltavista sammelt, verarbeitet und nutzt Daten“. In diesem Jahr erzielt Deltavista zum ersten Mal nach Jahren der Investition ein ausgeglichenes Ergebnis.
2005	Die 2004 formulierte Strategie wird konsequent weiter verfolgt: • Das Datensammeln wird verstärkt durch die Übernahme von vier marktführenden Datenproduzenten in Österreich und in der Schweiz. • Die Datenqualität wird erhöht durch die Verdopplung des Datenpflegeteams von 10 auf 20. • Der Datenmehrwert wird erhöht durch die Kooperation mit Informa Unternehmensberatung GmbH und die daraus resultierenden Entwicklungen von neuen, hochwertigen und marktführenden Scoring-Produkten.

Der Erfolg der Strategie wird bestätigt durch das starke Umsatzwachstum in allen

Ländern, die Verstärkung aller Teams durch erfahrene Führungskräfte und das Realisieren eines respektablen Jahresgewinnes.

2006 Die Strategie wird verfeinert:

- neue Datenpools und Kundenverträge verdoppeln den Datenbestand
- neue Software-Entwicklungen verbessern maßgeblich die Datenverarbeitung
- neu entwickelte Scores sind in ersten Tests sehr erfolgreich
- eine Serie identischer Standardprodukte wird für alle Länder definiert.

2007 Die verfeinerte Strategie wird umgesetzt:

- allgemeine Pooling- und Identifikationsprodukte werden definiert und implementiert.
- B2C/B2B-Decisionprodukte, die auf Score-Entwicklungen basieren, werden in allen Ländern eingeführt.³⁹¹

Die Datenbank umfasst nach eigenen Angaben über acht Millionen Datensätze und ist die größte österreichische Datenbank diesbezüglich. Neben der Bonitätsabfrage wird der Benutzer auch mit Firmenprofilen von der weltweit größten Auskunft Dun & Bradstreet versorgt. Diese Kooperation endete jedoch mit Ende 2008. Seit April 2009 bietet Deltavista nun eigene (Firmen-)Bonitätsauskünfte an.

Deltavista hat derzeit österreichweit über 30 Inkassobüros unter Vertrag welche regelmäßig aktuelle Inkassofälle (-übergaben) an eine gemeinsame Datenbank einmelden.

Der Vorteil für die Inkassobüros ist kein unmittelbar finanzieller sondern der Zugriff auf die gemeinsame Datenbank um dadurch ihren eigenen Kunden zusätzlich zur Inkassodienstleistung auch die bestmöglichen Bonitätsauskünfte zu erteilen.

Der Umsatz beläuft sich in Österreich seit der Gründung im einstelligen € Millionenbereich. Derzeit nutzen über 500 Kunden in Österreich die Dienste von Deltavista wobei die größten Umsatzbringer Unternehmen aus dem Banken und Leasingbereich, der Telekommunikation, der Energieversorger und dem Versandhandel darstellen.³⁹²

³⁹¹ <http://www.deltavista.com/content/view/29/54/lang,ge/>

³⁹² Genauere Daten werden aufgrund von Geschäftsgeheimnissen nicht zur Verfügung gestellt

Aufbau einer Firmenauskunft (Muster):



Deltavista Credit Check - Business

Abgefragt von Anna Maria Testa vom 17.12.2008 14:10 Nr. 4175237

Entscheidung		
Gesucht	Gefunden	Beurteilung
Phantasy GmbH ABC-Strasse 77 8700 Küsnacht Schweiz	Phantasy GmbH ABC-Strasse 77 8700 Küsnacht Schweiz	 ROT
Beurteilung		Score 250 My Limit CHF 0 My Rating D---

Basisdaten		
Firmenname	Phantasy GmbH	Zweck
Firmensitz / Domizil	ABC-Strasse, 8700 Küsnacht	Kontakt
Mutterhaus	n.a.	
Rechtsform	Gesellschaft mit beschränkter Haftung	
CH Nummer	CH-950.0.000.019-9	
Handelsregisterort	Küsnacht	
Firmenstatus	AKTIV	
Gründungsdatum	01.01.2005	
Nominalkapital	CHF 20'000.-- (voll libriert)	
Branche	Industrie 7420H Sonstige technische Beratung und Planung	
Mitarbeiter	n.a.	
Unternehmensgrösse i	klein	
Revisionsstelle	n.a.	

Entscheidungsmatrix		
Element	Wert	Beurteilung
Score	250	 rot
Trafferart	Traffer Kapitalgesellschaft	 grün
Firmenstatus	aktiv	 grün
Unternehmensführung und Management		 grün
Tage seit Domizilwechsel	n.a.	 grün
Tage seit Namenswechsel	n.a.	 grün
Tage seit Revisionswechsel	n.a.	 grün
Sacheinlagen	ja	 gelb
Ähnlichkeitstrafer	1	 gelb
Entscheidung		 ROT
Entscheidungsgrund	Score (250)	



11.1. Rechtliche Beurteilung

Die Datenbank der Firma „Deltavista“ umfasst einerseits Firmenauskünfte in sehr komprimierter, übersichtlicher und entscheidungsrelevanter Form (siehe Beispiel) als auch eine integrierte Privatkundendatenbank mit über 8.000.000 Einträgen. Diese Datenbank unterliegt der Vorabkontrolle iSd § 18 Abs 2 Z 3 DSG 2000 da sie die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Inhalt hat und darüber hinaus in Form eines Informationsverbundsystems geführt wird (§ 18 Abs 2 Z 4 DSG 2000). Dies wurde auch von der DSK bestätigt.

Die darin eingemeldeten und weitergegebenen Bonitätsdaten von Privatpersonen unterliegen den schutzwürdigen Geheimhaltungsinteressen nach § 1 DSG 2000. Aus der Empfehlung der DSK³⁹³ ist ersichtlich, dass der Gesetzgeber von der grundsätzlichen Zulässigkeit von Sammeln bonitätsrelevanter Daten im Rahmen der Tätigkeit als Auskunftsei über Kreditverhältnisse ausgeht. Gesammelte Exekutionsdaten sind aufgrund der gesetzlichen Anordnung in den §§ 71, 71a EO öffentlich und daher besteht kein schutzwürdiges Interesse an deren Geheimhaltung.

In Bezug auf gesammelte und eingemeldete Inkassodaten aufgrund des bestehenden Rahmenvertrages zwischen Deltavista und den Inkassounternehmen kann diese Verwendung aufgrund der bestehenden Gewerbeberechtigung nach § 152 GewO iSd § 7 DSG 2000 als zulässig angesehen und unter § 8 Abs 1 Z 4 DSG 2000 („überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten“) subsumiert und rechtliche legitimiert werden.

Die Firmenauskünfte werden derzeit selbst recherchiert und auch in das System entscheidungsfertig integriert. Hiefür gilt rechtlich, dass die Unternehmensdaten aus dem Firmenbuch als eine öffentlich zugängliche Datenbank kein schützenswertes Geheimhaltungsinteresse iSd § 1 DSG 2000 mehr aufweisen. Bilanzinformationen über Jahresabschluss und Lagebericht (eventuell auch Corporate Governance-Bericht) liegen ebenfalls bei den Firmenbuchgerichten zur Einsicht auf. Kapitalgesellschaften sind nach § 277 UGB verpflichtet diese beim jeweiligen Firmenbuchgericht (unter Androhung von Zwangsmaßnahmen und Strafbestimmungen gemäß § 283 UGB) zu hinterlegen. Ein schutzwürdiges Geheimhaltungsinteresse iSd § 1 DSG 2000 ist daher nicht erkennbar.

Das darin enthaltene Ratingurteil ist jedoch als Prognose einzustufen weil es über die Wahrscheinlichkeit der vertragsgemäßen Erfüllung von Liefer- und Leistungsverpflichtungen

³⁹³ GZ K21.773/009-DSK/2007 vom 7. Mai 2007

„urteilt“. Damit ist aber keine Garantie über den Eintritt eines bestimmten Erfolgs verbunden. Infolge des Prognosecharakters und der zukünftigen Unsicherheit ist dieses jedoch nicht als Tatsachenbehauptung zu qualifizieren und zum Zeitpunkt der Festsetzung als richtig oder falsch zu qualifizieren ist, dem Beweis nicht zugänglich. Sie sind deshalb als ein subjektives Werturteil, eine Meinungsäußerung über wie wirtschaftliche Bonität eines Unternehmens zu sehen und sind in dieser Hinsicht einer gerichtlichen Überprüfung in Hinblick auf die inhaltliche Richtigkeit, entzogen.

Nachdem es in der Vergangenheit immer wieder auch zu Anständen aufgrund unrichtiger und veralteter Daten gekommen ist und auch trotz prinzipieller Richtigkeit der Daten Waren und Dienstleistungen Betroffenen vorenthalten wurden, hat der OGH in seiner E³⁹⁴ erstmals ausdrücklich ausgesprochen, dass es jedermann/-frau frei steht Widerspruch iSd § 28 Abs 2 DSG 2000 zu erheben, und seine Daten in einer öffentlich zugänglichen Datei jederzeit auch ohne Begründung seines Begehrens löschen lassen kann. Trotz eines geschlossenen Benutzerkreises anerkannte der OGH diese nicht als „nicht-öffentliche“ Datei und verglich sie mit dem Zugriff auf das Grundbuch weil auch dort Entgeltlichkeit vorhanden ist. Diese Sichtweise mag im Prinzip richtig sein, geht nur leider in diesem Falle völlig am Kern des Problems vorbei. Ein Grundbuch/Firmenbuch kann und darf von jedermann/-frau eingesehen werden. (§ 7 GBG bzw. § 34 Abs FBG und § 9 UBG) Ein Zugriff auf eine Bonitätsdatenbank ist jedoch auf keinen Fall in dieser Art und Weise möglich. Bei öffentlichen Datenbanken besteht daher ein Rechtsanspruch auf Einsichtnahme. Dies würde bei Privatunternehmen zu einem Kontrahierungszwang führen welcher in dieser Form nicht existent ist.³⁹⁵ Hierzu ist zuerst die Notwendigkeit (im weiteren Sinn ist damit das überwiegend berechtigte Interesse iSd § 8 Abs 1 Z 4 DSG 2000 gemeint) nachzuweisen, Rahmenverträge zwischen dem Anbieter (Deltavista) und dem Kunden abzuschließen und eine Vertraulichkeitserklärung zu unterzeichnen. „Öffentlich zugänglich“ wird in mehreren Gesetzen³⁹⁶ als „die Möglichkeit von jedermann unter den selben Bedingungen Einsicht in eine Datei zu nehmen und davon Kenntnis erlangen zu können“ bezeichnet. Man muss daher den Begriff „öffentlich zugängliche Datei“ eng auszulegen haben, sodass darunter allgemein für jedermann und jederzeit zugängliche Datenbanken (wie zB Herold, Wikipedia, Ediktsdatei, etc) fallen und

³⁹⁴ OGH 1.10.2008, 6 Ob 195/08g

³⁹⁵ Zutreffend *Forgo*, Das Widerspruchsrecht nach § 28 Abs 2 DSG 2000, JusIT 1/2009, 18ff

³⁹⁶ zB § 16 GesundheitstelematikG, § 43 Abs 1 InvFG, § 54 AWG 2002, § 21b Abs 1 Z 4 BWG, § 243b Abs 1 Z 2 UBG, § 18 Abs 1 VerwGesG 2005; weiters ist jedoch darauf hinzuweisen, dass es in der österreichischen Rechtsordnung keinen einheitlichen Begriff von „Öffentlichkeit“ gibt – zum UrhR *Schumacher in Kucsko* (Hrsg), Urheberrecht (2008), § 8 UrhG, 178

nicht jegliche Dateien, auf die nur ein eingeschränkter, individualisierter Personenkreis Zugriff hat.

§ 28 Abs 1 DSG 2000 hingegen stellt auf den Sonderfall ab, dass die Datenanwendung zwar zulässig ist, eine aus der spezifischen Situation des Betroffenen heraus vorgenommene Interessenabwägung aber zu Gunsten des Betroffenen ausfällt. Der Rechtsweg des Betroffenen bei Nichtbeachtung des Widerspruchs führt im Fall eines Auftraggebers des öffentlichen Bereichs über die Datenschutzkommission zu den Gerichtshöfen des öffentlichen Rechts; im privaten Bereich sind für die Durchsetzung des Widerspruchsrechts die ordentlichen Gerichte berufen. Ein Widerspruch steht nur bei Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen zu, die sich aus einer besonderen Situation ergeben müssen.

Die Aussagekraft solcher Dateien wird daher weiter eingeschränkt und die Verlässlichkeit ebenso reduziert. Ein daraus resultierendes Spannungsfeld von § 152 GewO und § 28 Abs 2 DSG 2000 ist imminent und bedarf einer dringenden Klärung im Sinne der Rechtssicherheit sowohl für Auskunftfeien als auch der kreditgewährenden Wirtschaft.

12. Datengeheimnis (§ 15 DSG 2000)

Die §§ 10 und 15 DSG 2000 muss man im Konnex betrachten da jedes mit dem anderen in dessen Anwendungsbereich verbunden ist.

Diese Verschwiegenheitspflicht gilt jedoch nicht kraft Gesetzes, sondern ausschließlich aufgrund vertraglicher Verpflichtung des Mitarbeiters, des unselbständig Beschäftigten, mit seinem Arbeitgeber, dem Rechtsträger.³⁹⁷ Sie stellt jedoch nach Ende des Dienstverhältnisses keine Konkurrenzklausel dar und umfasst auch die widerrechtliche Benutzung und Verwertung der Daten durch den (ehemaligen) Arbeitnehmer selbst.³⁹⁸

Unter Mitarbeiter werden dabei Arbeitnehmer bzw. Dienstnehmer und Personen in einem arbeitnehmerähnlichen bzw. dienstnehmerähnlichen Verhältnis verstanden. Als Entscheidungsmerkmale dienen dazu vor allem die wirtschaftliche Abhängigkeit, die Einschränkung der Entschlussfähigkeit, die Verpflichtung zur persönlichen Arbeitsleistung und die Festlegung der Arbeit durch Fremdbestimmung. Auch Volontäre, Ferialpraktikanten und Aushilfskräfte fallen darunter.³⁹⁹

Sowohl Auftraggeber als auch Dienstleister haben die erforderlichen Datensicherheitsmaßnahmen iSd § 14 DSG 2000 zu treffen.^{400 401} So wie das Bankgeheimnis kein Geheimnis der Bank darstellt sondern eine Verschwiegenheitsverpflichtung, bedeutet das Datengeheimnis eine Verpflichtung zur Geheimhaltung. Ein Weitergabe/Übermittlung ist nur aufgrund einer ausdrücklichen Anordnung des Auftrags- oder Arbeitgebers zulässig.⁴⁰² Der Arbeitgeber darf derartige Anordnungen nur erteilen, wenn diese gesetzlich zulässig sind. Ungesetzliche Weisungen darf der Mitarbeiter nicht befolgen. Dies gilt sowohl für den privaten als auch den öffentlichen Bereich. Die im alten DSG normierte Bestimmung auch durch die „Anordnung eines Vertreters“ zulässige Bestimmung wurde gestrichen. Zweck dieser Bestimmung ist, die genaue Verantwortlichkeit für die Übermittlung von Daten klarzustellen.

³⁹⁷ Weiss, Bankgeheimnis und Datenschutz, EDVuR 1994, 86

³⁹⁸ OGH 4.12.1996, 9 Ob A 2154/96x

³⁹⁹ Jahnelt, Aktuelle Fragen des Datenschutzrechts, 101; Dohr/Pollirer/Weiss, DSG², § 15 Anm 4

⁴⁰⁰ Auf weitere Einzelheiten in Bezug auf Organisationsmaßnahmen und Technikstandards muss hier verzichtet werden

⁴⁰¹ Siehe zB die Auflagen der DSK vom 25.2.2000, 202.001/3-DSK/00; DSK vom 22.01.2002, K202.017/002-DSK/2002; DSK vom 05.4.2006, K202.046/0012-DSK/2006

⁴⁰² Ähnliches gilt auch für die Amtsverschwiegenheit und Berufsgeheimnisse da sie ebenfalls personenbezogen sind; vgl. dazu Wieser, Art 20 Abs 3, in Korinek/Holoubek, Österr. Bundesverfassungsrecht (Loseblatt, 1999ff) Rz 39 mwN; Knyrim/Heidinger, Die Zulässigkeit der Bekanntgabe personenbezogener Daten an Untersuchungskommissionen, ZfV 2005/1155.

Im öffentlichen Bereich ist das Datengeheimnis durch das Amtsgeheimnis gewährleistet, wogegen im privaten Bereich die gesetzlichen Bestimmungen des § 15 DSG von Bedeutung sind. Das Verbot wird nicht nur die Weitergabe einer als gesichert geltenden Information, sondern auch von bloßen Vermutungen umfassen.⁴⁰³ Der Hinweis auf die „sonstigen gesetzlichen Verschwiegenheitspflichten“ drückt aus, dass das Datengeheimnis *kumulativ* neben sonstigen gesetzlichen Verschwiegenheitspflichten wie Amtsgeheimnis, Ärztegeheimnis, Anwaltsgeheimnis, Bankgeheimnis, etc auftritt.⁴⁰⁴ In diesem Zusammenhang ist auf die ausdrücklichen Bestimmungen der §§ 84 Abs 1 Satz 2 AktG sowie § 99 AktG für Vorstands- und Aufsichtsratsmitglieder hinzuweisen welche angehalten sind, über vertrauliche Angaben Stillschweigen zu bewahren.⁴⁰⁵

Nicht als eine die Übermittlung ausschließende gesetzliche Verschwiegenheitspflicht iSd §§ 7 und 8 DSG 2000 ist das Datengeheimnis anzusehen, da dieses eine für die Beschäftigten eines Unternehmens wirkende Geheimhaltungspflicht darstellt, aber nicht für das Unternehmen selbst.⁴⁰⁶

Arbeitgeber haben daher ihre Mitarbeiter vertraglich zur Einhaltung des Datengeheimnisses zu verpflichten und über Datenschutz im Allgemeinen und den Ablauf der Datenverarbeitung im eigenen Unternehmen zu belehren.

12.1. Umfang der Verschwiegenheitspflicht

Personell: Personen, die aufgrund ihrer berufsmäßigen Beschäftigung Daten anvertraut oder zugänglich gemacht worden sind (§ 15 Abs 1 DSG 2000)

Sachlich: Übermittlung von Daten nur aufgrund einer ausdrücklichen Anordnung des Auftrag- oder Arbeitgebers (§ 15 Abs. 2 DSG 2000)

Zeitlich: Gilt weiter unabhängig von der Beendigung der Tätigkeit (§ 15 Abs 2 letzter Satz DSG 2000)

⁴⁰³ Vgl OGH 13 Os 174/81 = SSt 53/4: „Wollte man nur die Bekanntgabe einer unverrückbar feststehenden Tatsache als Geheimnisverletzung ansehen, so wären der Umgehung des Geheimnisschutzes Tür und Tor geöffnet; es würde jeder, der ein Amtsgeheimnis straflos preisgeben will, seine Bekanntgabe in eine Vermutung kleiden, aber durchblicken lassen, dass an deren Richtigkeit kaum zu zweifeln sei.“

⁴⁰⁴ Duschaneck/Rosenmayr-Klemenz, DSG 2000, 71

⁴⁰⁵ Dazu ausführlich Nowotny, in Doralt/Nowotny/Kalss, AktG (2003) § 84 Rz 12, sowie Kalss zu § 99 Rz 21; Kastner/Doralt/Nowotny, Gesellschaftsrecht, 5. Aufl, 263; Lutter, Information und Vertraulichkeit im Aufsichtsrat³ (2006), 172

⁴⁰⁶ ÖZW, 1979/1,17

12.2. Verpflichtungserklärung

Für Personen, denen aufgrund ihrer berufsmäßigen Beschäftigung Daten anvertraut oder zugänglich gemacht werden, sind wenn sie nicht schon von Gesetzes wegen dazu verpflichtet sind, haben eine Datenübermittlung nur durch vertragliche Verpflichtung aufgrund einer Anordnung durchzuführen.

Grundsätzlich herrscht auch im Arbeitsvertragsrecht die privatrechtliche Formfreiheit und dient Schriftlichkeit demnach nur zu Beweis Zwecken und diese wird hier vom Gesetzgeber NICHT ausdrücklich verlangt und daher ist eine ausdrückliche mündliche Zusicherung als ausreichend anzusehen. Es wird jedoch unter eigenen Angestellten sowie Geschäftspartnern dringend empfohlen die Verpflichtungserklärung in Schriftform festzuhalten und auch den Personenkreis nicht zu klein zu halten.

Beispiel einer Verpflichtungserklärung:⁴⁰⁷

„Ich verpflichte mich, Daten aus Datenverarbeitungen, die mir zugänglich geworden sind, unbeschadet sonstiger Verschwiegenheitspflichten, nur auf Grund einer ausdrücklichen Anordnung des Auftrag- oder Arbeitgebers zu übermitteln.

Ich erkläre hiermit ausdrücklich, dass ich Daten aus Datenverarbeitungen nur auf Grund der Anordnung gemäß § 15 Abs 3 DSG 2000 übermitteln werde und dass ich das Datengeheimnis im Sinne des § 15 Abs 1 DSG 2000 auch nach Beendigung meines Dienstverhältnisses einhalten werde.

Gleichzeitig nehme ich zur Kenntnis, dass ein Verstoß gegen das Datengeheimnis nicht nur arbeitsrechtliche Folgen (zB Entlassung) haben kann, sondern auch strafrechtliche geahndet werden und allenfalls schadenersatzpflichtig machen kann“

Die Unterlassung der Einholung einer Verpflichtungserklärung von Seiten der Auftraggeber oder Dienstleister, könnte eine Verwaltungsübertretung nach § 52 Abs 2 Z 4 DSG 2000

⁴⁰⁷ Aus Duschaneck, Datenschutzrecht im Unternehmen, 69

darstellen, nämlich ein gröbliches Außerachtlassen von Sicherheitsmaßnahmen nach § 14 DSG 2000.⁴⁰⁸

Konsequenzen:

Klare, personelle Beschreibung der Berechtigungen zu Übermittlungen

Formulierungen der Übermittlungsaufträge als Organisationsaufgabe

Zugriffsberechtigungen und Aufgabendurchführung sind aufgrund der gesetzlichen Bestimmungen zu treffen und auch zu überprüfen

12.3. Bruch der Verschwiegenheitspflicht

- Verwaltungsrechtliche (§ 52 DSG 2000) mit einer Verwaltungsstrafe bis zu € 18.890,-- oder strafrechtliche Konsequenzen (§ 51 DSG 2000 bzw §§ 118a ff, 148a StGB)
- Schadenersatz
- Entlassung (ergibt sich aus § 27 Z 1 AngG wonach stRsp bei Preisgabe von Betriebs- und Geschäftsgeheimnissen ein Fall von „Untreue“ und „Vertrauensunwürdigkeit“ vorliegt welcher einen wichtigen Grund zur Entlassung darstellt)
- Versetzung⁴⁰⁹

⁴⁰⁸ So *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz, § 15 Anm 6

⁴⁰⁹ In Anlehnung an RWZ 1993/4, *Weiss/Pollirer*, Datenschutz in der Wirtschaft, 118

13. Offenlegungs- und Informationspflichten des Auftraggebers

Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offen zu legen, so dass den Betroffenen die Verfolgung ihrer Rechte möglich ist. (§ 25 Abs 1 DSG 2000). Dies betrifft vor allem Fälle in denen keine Registriernummer (DVR Nummer) geführt wird, weil es sich nicht um meldepflichtige Datenanwendungen handelt. Konkret bedeutet dies, dass Name und Anschrift des Auftraggebers anzuführen sind und die bloße Verwendung von Postfächern oder Telefonnummern nicht ausreicht.

Da im § 23 DSG 2000 Hinweise auf die Form der „Offenlegung“, die einzuhaltende Frist, Möglichkeiten der Verweigerung bei schikanösen Anfragen usw. fehlen, und auch keine Durchsetzung vorgesehen ist, bleibt dem Fragesteller nur die Beschwerde an die DSK gem. § 30 Abs DSG 2000 im Falle ungerechtfertigter Verweigerung. Dem Auftraggeber steht somit ein gewisser Spielraum für die Erledigung einer Anfrage zur Verfügung.

Eine Verletzung der Offenlegungspflicht stellt allerdings eine Verwaltungsübertretung iSd § 52 Abs 2 Z 3 DSG 2000 dar. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registriernummer des Auftraggebers anzuführen.

Eine nicht unumstrittene Regelung betrifft in § 24 DSG 2000 die Informationspflicht des Auftraggebers, den Betroffenen auch ohne Antrag bei Ermittlung von Daten in geeigneter Weise über den Zweck der Datenanwendung für die Daten ermittelt werden, über Namen und Adresse des Auftraggebers zu informieren, sofern diese Informationen den Betroffenen nach den Umständen des Falles nicht bereits vorliegen.⁴¹⁰ Dies bedeutet jedoch nicht eine Verdoppelung der Meldepflicht an das DVR in Form einer zusätzlichen Pflicht zur „Meldung an den Betroffenen“. „Vor dem Hintergrund des Bestehens einer Registrierungspflicht muss vielmehr der Sinn einer zusätzlichen Informationspflicht darin gesehen werden,“ dass dem Betroffenen immer dann, „wenn ihm diese Information nicht bereits vorliegt“, der Hinweis gegeben wird, dass seine Daten von einem bestimmten Auftraggeber für einen bestimmten Zweck verarbeitet und er in die Lage versetzt wird, sich – falls er dies wünscht – aller Hilfsmittel zu bedienen, um „ordnungsgemäß und umfassend informiert zu werden.“⁴¹¹ Der Informationspflicht des Auftraggebers aus Anlass der Datenermittlung entspricht kein

⁴¹⁰ Erwägungsgrund 38 der DS-RL: „Der Betroffene soll über das Vorhandensein einer Verarbeitung erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert werden.“

⁴¹¹ EB zu § 24 in Duschaneck/Rosenmayr-Klemenz, DSG-RV, ecolex 1999, 364

durchsetzbarer Rechtsanspruch des Betroffenen auf Erhalt dieser Informationen. Sie setzt aber auch kein besonderes Ersuchen des Betroffenen voraus. Bei Vorliegen der gesetzlichen Voraussetzungen hat der Auftraggeber aktiv zu werden.⁴¹²

Darüber hinaus gehende Informationen sind „in geeigneter Weise“ dann bekannt zu geben, wenn diese für eine Verarbeitung nach Treu und Glauben erforderlich sind. Dies ist beispielsweise dann der Fall, wenn ein Widerspruchsrecht nach § 28 DSG 2000 (siehe unten) besteht oder es nach den Umständen des Falles nicht klar erkennbar ist, ob eine Verpflichtung zur Beantwortung der gestellten Fragen besteht oder wenn Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist. Keine Informationspflicht besteht bei Datenanwendungen welche nicht meldepflichtig sind.

Die Information darf entfallen (§ 24 Abs 3 DSG 2000), wenn die Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt wurden, wenn

- die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist, oder
- die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist, oder
- angesichts der Unwahrscheinlichkeit einer Beeinträchtigung die Kosten der Information einen unverhältnismäßigen Aufwand erfordern.

Auch aus Gründen woraus aufgrund allgemeiner Lebenserfahrung auszugehen ist, dass der Einsatz der Datenverarbeitung notwendig ist wie zB bei Schaltergeschäften in Kreditinstituten, bei Buchungen im Reisebüro usw. wird sich eine diesbezügliche Information erübrigen.

Zusammenfassend kann damit gesagt werden, dass es für die Informationspflicht in der konkreten Situation darauf an kommt, ob die Information über Zweck der Datenanwendung und Identität des Auftraggebers bereits vorliegt. Dies wird zB dann der Fall sein, wenn der Betroffene bereits Informationen mittels eines Fragebogens bekannt gab, jeden Zweifel darüber ausschließen, dass die Daten vom Datenermittler für einen vom Betroffenen einsichtigen Zweck, verarbeitet werden. In diesem Falle würde keine Informationspflicht

⁴¹² *Duschanek*, Neuerungen und offene Fragen im DSG 2000, ZfV 2000/1303, 533

bestehen. Werden jedoch die Daten durch Übermittlung aus anderen Anwendungen ermittelt, so wird der Betroffene in der Regel keine Informationen darüber haben und würde eine Informationspflicht des Auftraggebers auslösen wenn nicht eine der o.a. Ausnahmen zum Tragen kommt. Durch die vom Gesetz geforderte Prüfung ob und welche Information im Einzelfall zu geben ist, wird der Auftraggeber verpflichtet oft einen komplexen Sachverhalt genauestens zu prüfen und sodann nach bestem Wissen und Gewissen dementsprechend zu entscheiden.⁴¹³

⁴¹³ *Jahnel*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 02/2000, 53

14. Die Rechte des Betroffenen

Der VfGH hat dazu ausgeführt:⁴¹⁴ „*Das Recht auf Geheimhaltung bezieht sich sowohl auf nicht automationsunterstützte als auch auf automationsunterstützt verarbeitete Daten (während die Rechte auf Auskunft, Richtigstellung und Löschung nur automationsunterstützt verarbeitete Daten um Gegenstand haben).*“

Entgegen der Auffassung des VfGH vertritt der OGH⁴¹⁵ eine andere Auffassung zu diesem Thema und unterscheidet nicht zwischen dem Anspruch auf Geheimhaltung gem § 1 Abs 1 DSG 2000 und den Rechten auf Auskunft, Richtigstellung und Löschung iSd § 1 Abs 3 DSG 2000: Obwohl „*das Gesetz dies weder in § 1 DSG idgF noch in den Begriffsbestimmungen des § 4 DSG 2000 ausdrücklich zum Ausdruck bringt*“, sei es „*nach der systematischen und teleologischen Interpretation nicht zweifelhaft, dass das Recht auf Datenschutz gem § 1 leg cit nur solche personenbezogenen Daten (§ 4 Z 1 leg cit) betreffen kann, die in einer Datei aufscheinen, also nach der gesetzlichen Begriffsdefinition in einer strukturierten Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind (§ 4 Z 6 DSG 2000)*“.

Dabei verkennt er jedoch, dass § 1 Abs 1 DSG 2000 allgemein von „Daten“ jedoch Abs 3 von „Daten, die zur Verarbeitung in manuell geführten Dateien bestimmt sind, spricht. Der OGH begründet sein Auslegungsergebnis mit dem Erfordernis einer richtlinienkonformen Interpretation des DSG 2000 iSd Art 3 Abs 1 der Datenschutz RL wo im gesamten Anwendungsbereich des Grundrechts auf Datenschutz (inklusive § 1 Abs 1 DSG 2000) Daten aus zumindestens einer manuellen „Datei“ im Sinne von Art 3 Abs 1 Datenschutz RL vorliegen muss andernfalls drohe auch (insbesondere im Hinblick auf Akten aus behördlichen Verfahren und Urkunden) eine „uferlose Ausweitung des Datenschutzes“. Dieser Rechtsansicht wird jedoch von der hL nicht gefolgt.⁴¹⁶

Auf die Rechte der §§ 26 (Auskunftsrecht), 27 Richtigstellungs- oder Löschungsrecht, 28 Widerspruchsrecht DSG 2000 kann der Betroffene iSd § 1444 ABGB verzichten. Es ist weder ausdrücklich die Unverzichtbarkeit dieser Rechte normiert, noch geht dies aus dem Zweck der §§ 26 bis 28 DSG 2000 hervor. Grenzen sind die allgemeinen Grundsätze zum Verzicht welche zB einen Verzicht auf die Geltendmachung zukünftiger Ansprüche aus rechtswidrigen

⁴¹⁴ VfGH 12.10.1989, VfSlg 12.194/1989

⁴¹⁵ OGH 28.6.2000, 6 Ob 148/00h; in diesem Sinne auch OGH 25.6.2002, 1Ob 109/02i sowie OGH 13.2.2003, 8 Ob 4/03a wobei die zwei letztgenannten E eine definitive Klärung vermissen lassen

⁴¹⁶ *Rosenmayr-Klemenz*, Zum Schutz manueller Daten durch das DSG 2000 Gleichzeitig eine Bemerkung zum Beschluss des OGH vom 28.6.2000, 6 Ob 148/00h = ÖJZ 2001/1, ecolex 2001, 639

Handlungen nicht möglich machen.⁴¹⁷ Dieses Recht ist jedoch nicht Inhalt des Grundrechts auf Datenschutz doch kann ein berechtigter Widerspruch eine Lösungsverpflichtung auslösen und damit mittelbar eine Grundrechtsrelevanz aufweisen.⁴¹⁸

Im engen Zusammenhang mit der Zweckbindung bei der Datenverarbeitung als Ausdruck der umfassenden informationellen Selbstbestimmung sind auch die übrigen (im Vergleich zum DSG 1978) erweiterten Partizipationsrechte in der DS-RL und im DSG 2000 zu sehen.⁴¹⁹ Die Rechte auf Auskunft, Richtigstellung und Löschung werden nach § 1 Abs 3 DSG 2000 „nach Maßgabe gesetzlicher Bestimmungen“ eingeräumt. Dies bedeutet, dass der einfache Gesetzgeber die nähere Reichweite dieser Rechte und die Modalitäten ihrer Durchsetzung zu regeln hat(te).

Es handelt sich dabei um einen *Ausgestaltungsauftrag*, der dem Gesetzgeber einen gewissen Spielraum eröffnet und ihn ermächtigt, die Art und Weise der Geltendmachung der Betroffenenrechte zu regeln.⁴²⁰ Dieser bezieht sich jedoch nur auf die Modalitäten und ändert nichts daran, dass Beschränkungen dieser Rechte als Eingriff nach § 1 Abs 4 DSG 2000 auf ihre Rechtfertigung hin zu überprüfen sind.

Daher liegt auch kein Ausgestaltungsvorbehalt vor, der § 1 Abs 3 DSG 2000 zu einem Feinprüfungsgrundrecht machen würde, bei welchem die Bescheidprüfungszuständigkeit des VfGH durch jene des VfSG zur Gänze nach Art 133 Z 1 B-VG⁴²¹ ausgeschlossen wäre. Dies wurde vom VfGH im E VfSlg 11.548/1987 für das Grundrecht auf Auskunft und in VfSlg 12.768/1991 für das Grundrecht auf Richtigstellung und Löschung ausgesprochen. In VfSlg 16.986/2003 wurde die zum DSG 1978 ergangene Judikatur für § 1 Abs 3 DSG 2000 bestätigt.⁴²²

⁴¹⁷ Klang in Klang² VI 528; Rill in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, 81; zu beachten gilt auch das KSchG

⁴¹⁸ *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, Rz 72, 83ff; *Duschanek/Rosenmayr-Klemen*, 107ff, *Knyrim*, Datenschutzrecht, 228

⁴¹⁹ *Mayer-Schönberger/Zeger/Kronegger*, Auf dem Weg nach Europa, Zur Novellierung des DSG, ÖJZ 1998, 249; ausführlich *Brühmann/Zerdick*, Umsetzung, 559 sowie *Souhrada-Kirchmayer*, Vorschlag, 152ff

⁴²⁰ *Berka*, Grundrechte, Rz 484; *Öhlinger*, Verfassungsrecht, 6. Aufl, Rz 831; *Jahnel*, Datenschutzrecht, 252

⁴²¹ Art 133B-VG lautet: *Ausgeschlossen von der Zuständigkeit des Verwaltungsgerichtshofes sind:*

1. die Angelegenheiten, die zur Zuständigkeit des Verfassungsgerichtshofes gehören;

2. (Anm.: Aufgehoben durch Art. I Z 37 BVG, BGBl. Nr. 444/1974.)

3. die Angelegenheiten des Patentwesens;

4. die Angelegenheiten, über die in oberster Instanz die Entscheidung einer Kollegialbehörde zusteht, wenn nach dem die Einrichtung dieser Behörde regelnden Bundes- oder Landesgesetz unter den Mitgliedern sich wenigstens ein Richter befindet, auch die übrigen Mitglieder in Ausübung dieses Amtes an keine Weisungen gebunden sind, die Bescheide der Behörde nicht der Aufhebung oder Abänderung im Verwaltungsweg unterliegen und nicht, ungeachtet des Zutreffens dieser Bedingungen, die Anrufung des Verwaltungsgerichtshofes ausdrücklich für zulässig erklärt ist.

⁴²² *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000; FS Schäffer (2006), 326ff

14.1. Das Recht auf Auskunft

Das Auskunftsrecht ist als Ausführungsvorschrift zu dem in § 1 Abs 3 DSG 2000 verfassungsrechtlich gewährten Grundrecht einfachgesetzlich in § 26 DSG Abs 2 und 3 DSG 2000 verankerten Beschränkungen geregelt und begrenzt.⁴²³ Die Durchsetzung des Auskunftsanspruches aus dem privaten Bereich mithilfe der DSK zählt zu den seltenen Ausnahmefällen einer verwaltungsbehördlichen Entscheidung über zivilrechtliche Ansprüche.⁴²⁴

Die Auskunft hat die verarbeiteten Daten, deren Herkunft, allfällige Empfänger oder Empfängerkreise, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hierfür sowie auf Verlangen auch Namen und Adresse von Dienstleistern in allgemein verständlicher Form zu enthalten. Das Auskunftsrecht ist jedoch kein absolutes Recht sondern stehe aufgrund des § 1 Abs 3 sowie Abs 4 DSG 2000 unter einem doppelten Gesetzesvorbehalt. Wie in § 26 Abs 3 DSG 2000 auf einfachgesetzlicher Ebene ausdrücklich ausgeführt wird, hat dieses seine Grenzen in den berechtigten Interessen des Auftraggebers oder Dritten, sofern diese Interessen in einer konkreten Situation als „überwiegend“ zu werten seien. Bei der vorzunehmenden Interessensabwägung ist somit dem Interesse des Betroffenen auf Auskunftserteilung hinsichtlich des Ursprungs der personenbezogenen Daten, das Interesse des Auskunftspflichtigen auf Geheimhaltung gegenüber zu stellen.

Die nur wage und ungenaue Erteilung einer Auskunft über das Zustandekommen eines internen Ratings eines Unternehmens unter Berufung auf das Geschäftsgeheimnis (Erwägung zur Richtlinie Punkt 41), wird weder durch die DSK noch durch den VwGH unterstützt.⁴²⁵ Der darin genannten Wirtschaftsauskunftei wurde aufgetragen genau Angaben über befragte Lieferanten, Banken und Übermittlungsempfänger zu geben. Das Geschäftsgeheimnis darf nicht dazu führen, dass dem Betroffenen jegliche Auskunft verweigert oder die Empfänger ohne Interessensabwägung verschwiegen werden. Eine genaue Bezeichnung was genau bekannt gegeben bzw. übermittelt wurde, war jedoch nicht notwendig aber die Auskunft hat so konkret wie möglich zu erfolgen damit der Betroffene seine Berichtigungs- und

⁴²³ Wie wenig (private) Unternehmen als auch die öffentliche Hand in der Praxis mit dem Auskunftsrecht anfangen können, zeigt *Reichmann*, Das Auskunftsrecht nach dem Datenschutzgesetz 2000 – Eine Fallstudie, ZfV 2004/1529. Bei der an der Universität Graz durchgeführten Studie, waren nur 13 % der 39 gestellten Datenschutzanfragen korrekt beantwortet worden.

⁴²⁴ *Raschauer*, Allgemeines Verwaltungsrecht, Rz 507; *Antoniolli/Koja*, Allgemeines Verwaltungsrecht³, 109ff

⁴²⁵ GZ 121.049/0023-DSK/2005 vom 16.Dezember 2005 – bestätigt durch VwGH 23.1.2007 2006/06/0039; ebenso VwGH 19.12.2006 2005/06/0111

Löschungsrechte sowohl gegenüber der Quelle der Daten als auch gegenüber Übermittlungsempfänger durchsetzen kann.

Ob die Bekanntgabe von „Empfängerkreisen“ iSv § 26 Abs 1 DSG 2000 (in Übereinstimmung mit Art 12 DS-RL) welche dadurch eine ungenaue Verallgemeinerung darstellen, ausreichend ist, ist lt VwGH eine Auslegungssache im Einzelfall. Die Argumentation eine genaue Benennung sei nur notwendig wenn berechtigte Richtigstellungs- bzw. Löschungsinteressen vorhanden seien, wurde vom diesem ebenfalls nicht geteilt.

Bei wiederholtem Auskunftsbegehren darf die Auskunft ohne Einverständnis des Betroffenen nicht nur auf Veränderungen gegenüber seiner letzten Anfrage beschränkt werden. Dies ergibt sich sowohl aus dem Gesetzeswortlaut als auch aus dem Zweck der Vorschrift wo sich der Betroffene ein aktuelles und vollständiges Bild über die zu seiner Person gespeicherten Daten machen soll.

Das Auskunftsrecht nach dem DSG 2000 steht jedem von einer Datenverarbeitung Betroffenen zu und ist von seiner Nationalität, Wohnsitz oder Geschäftsfähigkeit unabhängig. Andere Personen können sich nicht auf § 26 DSG 2000 zur Auskunftserlangung berufen. Im Gegensatz zu den Auskunftsrechten nach dem Auskunftspflichtgesetz bzw. Art 20 Abs 4 B-VG die jedermann zustehen, der Auskünfte über Angelegenheiten des jeweiligen Wirkungsbereiches der Behörde wünscht.⁴²⁶

Durch die Trennung des Auskunftsrechts vom förmlichen Verfahren wie es das AVG kennt (§ 17 Akteneinsicht, § 13a allgemeine behördliche Auskunfts- und Beratungspflicht [Manuduktionspflicht]) kam es zu einer erheblichen Verbesserung der Rechtsposition des Betroffenen.

Eine allfällige Unterscheidung zwischen verpflichtender schriftlicher Auskunft im öffentlichen Bereich sowie möglicher mündlicher Auskunft im privaten Bereich ist nun nicht mehr vorgeschrieben und kann daher mit Zustimmung des Auftraggebers auch mündlich oder durch Zustimmung des Betroffenen auch mündlich mittels Einsichtnahme und Abschrift oder

⁴²⁶ § 1 Auskunftspflichtgesetz lautet: (1) Die Organe des Bundes sowie die Organe der durch die Bundesgesetzgebung zu regelnden Selbstverwaltung haben über Angelegenheiten ihres Wirkungsbereiches Auskünfte zu erteilen, soweit eine gesetzliche Verschwiegenheitspflicht dem nicht entgegensteht.

(2) Auskünfte sind nur in einem solchen Umfang zu erteilen, der die Besorgung der übrigen Aufgaben der Verwaltung nicht wesentlich beeinträchtigt; berufliche Vertretungen sind nur gegenüber den ihnen jeweils Zugehörigen auskunftspflichtig und dies insoweit, als dadurch die ordnungsgemäße Erfüllung ihrer gesetzlichen Aufgaben nicht verhindert wird. Sie sind nicht zu erteilen, wenn sie offenbar mutwillig verlangt werden.

Ablichtung erfolgen.⁴²⁷ Bei juristischen Personen sind deren vertretungsbefugte Organe berechtigt. Dies hat durch entsprechende Firmenbuch- oder Vereinsregisterauszüge von deren Seite belegt zu werden.⁴²⁸ Es können jedoch auch Dritte hiezu ermächtigt werden.

Als gewissermaßen Kompensation für die Belastung des Auftraggebers hat der Betroffene eine Mitwirkungsverpflichtung im Auskunftsverfahren in zumutbaren Ausmaß (§ 26 Abs 3 DSG 2000). Allgemein hat der Betroffene all jene Fragen des Auftraggebers zu beantworten, ohne deren Beantwortung die Auskunft nicht oder nur mit außerhalb der Relation stehenden Aufwendungen im Verhältnis zur Beantwortung, möglich wäre.⁴²⁹ Insgesamt soll die Mitwirkung ermöglichen, die Erledigung des Auskunftsbegehrens vorzubereiten und den Suchprozess abzukürzen. Der Auftraggeber ist jedoch nicht verpflichtet, seinerseits den Betroffenen, über die Eintragung im DVR hinausgehende Aufklärungen über Inhalt und Organisation seiner Datenverarbeitung zu geben. (abgesehen von der Verpflichtung zur Offenlegung gem § 23 Abs 1 DSG 2000)⁴³⁰

Die datenschutzrechtliche Auskunft ist nunmehr innerhalb von acht Wochen nach Einlagen des Begehrens zu erteilen obwohl Art 12 der Datenschutz RL vorschreibt, dass die Erteilung der Auskunft „ohne unzumutbare Verzögerung“ zu erfolgen hat und es daher fraglich ist, ob diese lange Frist eine ordnungsgemäße Umsetzung der Richtlinie bedeutet. Die DSK hat jedoch in ständiger Spruchpraxis anerkannt, dass eine spätere Auskunft eine ursprünglich nicht getätigte (vollständige) Auskunft nachträglich „sanieren“ kann. Die Nichteinhaltung der achtwöchigen Frist stellt zwar eine Verletzung des Rechts auf Auskunft dar, aber eine Nachholung der Auskunft bis zum Ende des Verfahrens vor der DSK lässt eine Sanierung zu.⁴³¹

Zuvor muss der Betroffene jedoch seine Identität nachweisen (zB durch Übersendung einer Ausweiskopie mit einem Vergleichsmuster seiner Unterschrift). Weiters ist festzuhalten, dass ein Auskunftsbegehren zulässigerweise auch per E-Mail gestellt werden kann. Dies hat die Datenschutzkommission schon in ihrem Bescheid, GZ K120.959/0009-DSK/2004 vom 16.

⁴²⁷ Mit Einverständnis des Betroffenen kann die Auskunft in folgenden Formen erteilt werden: mündlich, Akteneinsicht, Abschrift, Ablichtung, e-mail, Bildschirmfrage. Siehe hiezu *Dohr/Pollirer/Weiss*, DSG², Anm 18 zu § 26 und § 26 Abs 1 letzter Satz DSG 2000

⁴²⁸ Vgl. Stellungnahme des DSR zu Fragen des Identitätsnachweises, Soz. Si 1990, 50

⁴²⁹ DSK 14.12.1984, ZfVB 1987/2/3; OGH 13.12.1990, 6 Ob 24/90, EDVuR 1991/1/I, 71; OGH 25.3.1999, 6 Ob 292/98 d = EvBl 1999/154

⁴³⁰ *Duschanek*, DSG 2000, 101

⁴³¹ GZ K121.214/0006-DSK/2006 vom 11. Oktober 2006

November 2004, dargelegt. Auch eine Zustellung der Auskunft zu eigenen Händen erfüllt den Identitätsnachweis.⁴³²

Der VwGH vertritt jedoch die Auffassung, dass das Erfordernis, die erteilte Auskunft solle nur dem Betroffenen, und sonst niemandem zur Kenntnis gelangen, könne dadurch Genüge getan werden, dass eine Einschreibsendung mit dem Vermerk "eigenhändig" oder "Rückschein" bewirkt werde, könne nicht gefolgt werden.⁴³³

Durch eine eigenhändige Zustellung der begehrten Daten kann die Erfüllung des Erfordernisses des Identitätsnachweises bei der Stellung des Auskunftersuchens nämlich nicht ersetzt werden. Auch ein Hinweis auf vereinspolizeiliche Verwaltungsakten kann den von § 26 Abs 1 DSG 2000 geforderten Identitätsnachweis des Auskunftswerbers nicht ersetzen.⁴³⁴

Die Bekanntgabe des Geburtsdatums des Betroffenen ist nach § 26 Abs 1 DSG 2000 ein für den Nachweis der Identität bedeutsames Kriterium. Es ist jedoch nicht ausreichend, dass die bloße Bekanntgabe des Geburtsdatums bereits für den Identitätsnachweis nach § 26 Abs 1 DSG 2000 ausreicht. Der Nachweis der Identität hat in der Form zu erfolgen, die es dem Auftraggeber ermöglicht, die Identität des Auskunftswerbers mit der Person zu überprüfen, deren Daten Gegenstand der Auskunft sein soll. Im Hinblick auf die Zielsetzung des Gesetzes und zur Verhinderung von Missbrauch ist ein hoher Grad an Verlässlichkeit hinsichtlich des Identitätsnachweises zu fordern.

Derjenige, der sich als ein nicht zur berufsmäßigen Parteienvertretung Berufener nicht auf eine Vorschrift etwa wie § 8 Abs 1 RAO beziehen kann, gegenüber einem Auftraggeber durch die Übermittlung von Telefaxen in Form eines Auskunftersuchens, einer Vollmacht, aber ohne weiteren Nachweis über die Identität des Auskunftswerbers auftritt und derart ein Auskunftsbegehren unter Berufung auf eine Vollmacht stellt, ein Nachweis "in geeigneter Form" im Sinne des § 26 Abs 1 DSG 2000 nicht gelungen ist. In einem solchen Fall wäre vielmehr etwa die Vorlage eines Identitätsdokumentes in Form einer öffentlichen Urkunde (im Sinne der §§ 292 ff ZPO) zu fordern. Träten dies falls Zweifel über die Echtheit der

⁴³² Vgl. Rundschreiben des BKA 26.11.1987 zur Durchführung des Auskunftsrechts, 810.031/1-V/3/87

⁴³³ VwGH 18. 3.1992, Zl. 91/12/0007

⁴³⁴ Bekämpfter Bescheid der DSK GZ K120.980/0008-DSK/2004 vom 2. November 2004 vor dem VwGH 9.9.2008 2004/06/0221

öffentlichen Urkunde auf, so obläge es dem Auftraggeber (ähnlich wie in § 310 Abs 2 ZPO) Schritte zur Klärung der Echtheit der Urkunde zu setzen.⁴³⁵

Aber auch ohne Identitätsnachweis muss der Auftraggeber auf das Auskunftsbegehren reagieren, und zwar darauf hin, dass er den Betroffenen zur Erbringung eines Identitätsnachweises auffordert und ihm mitteilt, dass andernfalls eine Auskunftserteilung unterbleiben würde.

Auf diese Gelegenheit zur Verbesserung muss der Antragsteller aufmerksam gemacht werden nach dem Gebot der Datenverarbeitung nach Treu und Glauben (§ 6 Abs 1 Z 1 DSG 2000). Das Fehlen eines Identitätsnachweises führt also in jedem Fall zu einem Mehraufwand sowohl beim Auftraggeber als auch beim Auskunftswerber und in weiterer Folge zu einer Verzögerung der Erteilung einer Auskunft. Dies soll jedoch wie von vielen Betroffenen angenommen, keine Schikane darstellen sondern eine sinnvolle Sicherheitsvorkehrung um einen Missbrauch des Auskunftsrechts zur Informationsbeschaffung über Dritte auszuschließen⁴³⁶ weil eine Auskunft an Nichtberechtigte stellt eine Verletzung des Grundrechts auf Geheimhaltung personenbezogener Daten dar⁴³⁷ sowie eine Verletzung des Datengeheimnisses iSd § 15 Abs 1 DSG 2000. Kommt der Auskunftswerber der Verbesserung nicht nach, so liegt nicht einmal ein Auskunftsbegehren im Sinne des § 26 Abs 1 DSG 2000 vor.⁴³⁸

Für die Frage, wie ein „Identitätsnachweis iSd § 26 Abs 1 DSG 2000“ zu erbringen ist, ist darauf abzustellen, was geeignet ist, dass das Auskunftsbegehrens von der als Auskunftswerber bezeichneten und in ihrer Identität amtlich bestätigten Person herrührt. In der Rechtsprechung der Datenschutzkommission⁴³⁹ wurde mehrfach die Kopie eines amtlichen Lichtbildausweises als ausreichender Nachweis angesehen. Allerdings ausgehend von der Voraussetzung, dass der Auskunftsantrag unterschriftlich gestellt wird, sodass der Auftraggeber durch Vergleich der Unterschriften im Ausweis und auf dem Auskunftsbegehren mit hinreichender Sicherheit die Identität des Auskunftswerbers **und** die Echtheit des Auskunftsbegehrens erkennen kann.⁴⁴⁰ Wird ein Auskunftsbegehren für eine

⁴³⁵ vgl. *Dohr/Pollirer/Weiss*; DSG2, Anm. 8 zu § 26, die von einer generellen Unzulässigkeit von Auskunftsbegehren durch Fax-Übermittlung ausgehen, weil in diesem Fall kein zweifelsfreier Identitätsnachweis erbracht werden könne

⁴³⁶ DSB 2005, 30

⁴³⁷ VwGH 18.3.1992, 91/12/0007

⁴³⁸ DSB 2007, 33

⁴³⁹ zB Bescheid GZ K121.034/0006-DSK/2005, vom 2. August 2005

⁴⁴⁰ GZ K121.225/0001-DSK/2007 vom 2. Februar 2007

Personengesellschaft als Betroffene gestellt, so ist nur die Gesellschaft (beschwerde-) legitimiert nicht aber die dahinter stehenden (Privat-)Personen.⁴⁴¹

Vollständigkeitshalber sei noch angemerkt, dass § 26 DSG 2000 so zu verstehen ist, dass nach Abs 1 zwar nur ein „Betroffener iSd § 4 Z 3 DSG 2000“ ein Auskunftsrecht in dem Sinn hat, dass ihm der Inhalt von Daten (zu seiner Person) bekannt gegeben werden muss, dass nach dem Sinn des Abs. 4 aber darüber hinaus jedermann einen Anspruch auf Auskunft darüber hat, ob überhaupt Daten über ihn verarbeitet werden.

Die Datenschutzkommission hat wiederholt auch einen Anspruch auf eine so genannte „Negativauskunft“, dh die Auskunft, dass zum Auskunftswerber keinerlei Daten verarbeitet werden bzw. wurden (woraus sich – allerdings erst ex post – ergibt, dass der Auskunftswerber nicht Betroffener im Sinn des § 4 Z 3 DSG 2000 war) bejaht. Was in weiterer Denkweise wiederum bedeutet, dass jedermann einen Anspruch auf Auskunft hat ob Daten über ihn verarbeitet wurden.⁴⁴² Dies gebietet eine verfassungskonforme Auslegung des § 26 Abs 1 im Lichte des § 1 Abs 3 Z 1 DSG 2000.⁴⁴³ Durch die Erteilung einer Negativauskunft hat der Auftraggeber seine Auskunftspflicht erfüllt.

Eine namentliche Benennung von Mitarbeitern dem Betroffenen gegenüber ist, außer zB bei Verdacht einer völlig zweckfremden und nur im Interesse des Mitarbeiters gelegenen Datenverwendung, nicht erforderlich da im Hinblick auf die Rechtsverfolgung aus dieser Kenntnis kein Vorteil zu gewinnen ist.⁴⁴⁴

Das Auskunftsrecht gemäß § 26 DSG 2000 bezieht sich nur auf automationsunterstützte Verarbeitungen und manuelle Dateien. Ein Auskunftsrecht von personenbezogenen Daten in unstrukturierten Akteninhalten⁴⁴⁵ besteht genau so wenig aus Urkunden oder Briefen⁴⁴⁶ oder aus einem (psychologischen) Gutachten im Rahmen einer Stellenausschreibung.⁴⁴⁷ Auch der VfGH schloss sich der Meinung der DSK, dass ein Kopierakt keine manuelle Datei ist weil darunter nur eine strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind, zu verstehen ist. „Dem genügt ein nicht personenbezogener

⁴⁴¹ GZ K120.938/0003-DSK/2004 vom 7. Dezember 2004

⁴⁴² zB Bescheid der DSK, GZ K120.897/0003-DSK/2005 vom 20. Mai 2005; GZ 121.220/0001-DSK/2007 vom 2. Februar 2007)

⁴⁴³ GZ K121.220/0001-DSK/2007 vom 2. Februar 2007

⁴⁴⁴ GZ K121.038/0006-DSK/2005 vom 2. August 2005

⁴⁴⁵ GZ K120.688/20-DSK/00 vom 27. April 2000

⁴⁴⁶ GZ K120.737/002-DSK/01 vom 24. April 2001

⁴⁴⁷ VfGH 23.5.2005 2003/06/0021 nennt es einen „Kopienakt“

Papierakt nicht“ und bezieht sich dabei auf ErwG 27, der seiner Meinung nach Akten und Aktensammlungen vom Anwendungsbereich der Richtlinie ausschließt.⁴⁴⁸

Es stellen sich daher für jeden Auftraggeber folgende Fragen⁴⁴⁹ im Bereich des Auskunftsrechts:

- Welche Stelle in der Unternehmensorganisation entscheidet, ob eine Auskunft überhaupt erteilt werden muss oder darf ?
- Welche Stelle in der Unternehmensorganisation stellt die Auskunftsbereitschaft her ?
- Welche Stelle in der Unternehmensorganisation erteilt diese Auskünfte und in welcher Form ?
- Innerhalb welchen Zeitraumes ist eine Auskunftserteilung möglich ?
- Wird für die Auskunft ein Entgelt verlangt, wenn ja, in welcher Höhe ? (Materialkosten, Portokosten, anteilige EDV Kosten, Telefonkosten,...)

Die gesetzlichen Verschwiegenheitspflichten (im privaten Bereich etwa für Rechtsanwälte, Wirtschaftstreuhänder, Ärzte und auch das Bankgeheimnis) sind zu beachten und muss eine Auskunft nicht erteilt werden, wenn dadurch überwiegend berechnigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen gefährdet werden. Die Zulässigkeit der Auskunftsverweigerung ist im überwiegend berechtigten Interessen des Auftraggebers oder eines Dritte schriftlich zu begründen. Im Bereich des überwiegenden öffentlichen Interesses unterliegt sie der Kontrolle durch die Datenschutzkommission nach § 30 Abs 3 DSG 2000 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs 4 DSG 2000.

Desweiteren besteht ein Lösungsverbot für einen Zeitraum für vier Monaten ab Kenntnis eines Auskunftsbegehrens. Falls der Betroffene Beschwerde an die DSK erhebt, gilt das Lösungsverbot bis zum rechtskräftigen Abschluss des Verfahrens. (§ 26 Abs 7 DSG 2000) Hier ist Vorsicht geboten weil eine Löschung solcher Daten sowohl strafbar nach § 52 Abs 1 Z 4 DSG 2000 als auch nach § 126a StGB (Datenbeschädigung) ist wenn die Löschung in

⁴⁴⁸ VfGH 15.10.2005, B1590/03; VfGH 27.06.2006, B 482/05

⁴⁴⁹ RWZ 1993/8, Weiss/Pollirer, Datenschutz in der Wirtschaft II, 251

Kauf genommen wird. Fahrlässiges Handeln ist jedoch nicht strafbar. Das Auskunftsrecht ist nicht davon abhängig, dass der Betroffene eine Rechtswidrigkeit oder ein besonderes oder schutzwürdiges Interesse behauptet oder glaubhaft macht.⁴⁵⁰

Eine Auskunft im laufenden Jahr ist gratis⁴⁵¹ ansonsten dürfen € 18,89 bzw. sogar höhere tatsächliche Aufwendungen verlangt werden. Diese sind jedoch rückerstattet wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft zu einer Richtigstellung geführt hat.⁴⁵²

Aufgrund der jahrelangen Rechtsprechung der DSK, ersetzt eine Auskunft an die DSK nicht die Auskunft an den Auskunftswerber, da nur dieser selbst beurteilen kann, ob ihn die erteilte Auskunft zufrieden stellt oder nicht.⁴⁵³

Wiewohl jedoch auch gesagt werden muss, dass aufgrund der angeordneten Öffentlichkeit von Exekutionsdaten in den §§ 71, 71a EO ua kein Recht auf Geheimhaltung und rechtliches Interesse an einer Auskunft für die betreibende Partei besteht.⁴⁵⁴ Aufgrund § 73a EO haben Rechtsanwälte, Notare und Körperschaften des öffentlichen Rechts die Möglichkeit, elektronisch Einsicht in die Geschäftsbehelfe des Exekutionsverfahrens zu nehmen. Dabei können sie die Namensverzeichnisse der verpflichteten Parteien, die Liste der abgelegten Vermögensverzeichnisse und ergebnisloser Vollzugsversuche sowie die Pfändungsregister einsehen. Diese Einsicht ist jedoch nur zulässig, wenn dies zur Einleitung eines Rechtsstreites oder einer Exekution, zur Geltendmachung von Einwendungen gegen ein bereits eingeleitetes Exekutionsverfahren benötigt wird.

Die Auskunft darf nur im Falle gesetzlicher Verschwiegenheitspflichten sowie bei Gefährdung überwiegender berechtigter Interessen des Auftraggebers der Datenverarbeitung oder eines Dritten oder im überwiegenden öffentlichen Interesse verweigert werden. (§ 26 Abs 2 DSG 2000). Die Einschränkung in Bezug auf die berechtigten Interessen des Auftraggebers oder eines Dritten ist notwendig, um zu verhindern, dass unter Berufung des

⁴⁵⁰ GZ 120.709/8-DSK/00 vom 17. November 2000

⁴⁵¹ Vgl. dazu § 34 Abs 5 BDSG wo ein Entgelt verlangt werden kann, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Die Gratiserteilung soll sodann über ein mögliches persönliches „Datenaudit“ des Betroffenen beim Auftraggeber durch Abs 6 BDSG herbeigeführt werden

⁴⁵² RWZ 1993/8, *Weiss/Pollirer*, Datenschutz in der Wirtschaft II S. 250

⁴⁵³ DSB 2007, 32

⁴⁵⁴ GZ 121.217/0021-DSK vom 13. Dezember 2006

DSG die Preisgabe aller über den Betroffenen vorhandenen Informationen, die ja zB für den Auftraggeber Betriebsgeheimnisse darstellen können, erzwungen werden können.⁴⁵⁵

Wo liegt nun die Grenze des datenschutzrechtlichen Auskunftsbegehrens und wo fängt die „Willkür“ bzw. „Schikane“ an ? Wie andere zivilrechtliche Ansprüche unterliegt auch das Auskunftsrecht dem allgemeinen Schikaneverbot.⁴⁵⁶ In einem Richtungsweisenden Urteil des OGH⁴⁵⁷ welches sich noch auf das „alte“ Datenschutzgesetz 1978 bezog und dieses Urteil jedoch in meinen Augen auch auf das „neue“ DSG 2000 angewendet werden kann, wurde eindeutig dargelegt, dass der Betroffene einen Schaden nachweisen muss. Den Sachverhalt kurz zusammengefasst, wollte der Betroffene von einem Adressverlag wissen woher dieser seine Daten hätte und diesem sein akademischer Titel bekannt war obwohl dieser nicht im Telefonbuch aufschien. Der Adressverlag konnte (oder wollte auch nicht) jedoch nicht mehr eruieren woher er diese Information hatte. Der Betroffene klagte darauf hin den Adressverlag weil die erteilten Auskünfte unvollständig gewesen seien. Das Eventualbegehren belief sich auf öS 100.000 (€ 7.267,28) für den ideellen Schaden. Der OGH wies die Klage ab mit der Begründung, dass zwar die Auskunft mangelhaft und nicht vollständig gewesen aber eine Rekonstruktion des Sachverhaltes nicht möglich sei und daher Unmöglichkeit der Leistung vorliegt.⁴⁵⁸ Auch das Eventualbegehren wurde abgewiesen weil der Kläger kein Vorbringen erstattet hatte, worin den nun der ideelle Schaden bestehen soll. In der bloßen Verweigerung der Auskunft über die Herkunft des Doktorats könne ein solcher nicht gesehen werden. Im DSG 1978 war noch keine Verpflichtung zur Aufbewahrung von Daten vorgesehen aber auch trotzdem war diese aufgrund § 920 ABGB wo der Schuldner schon vor der Erfüllung verpflichtet war, alles in seiner Macht abzuwenden, was eine drohende Unmöglichkeit der Leistung bewirkt hätte und alles zu unterlassen was die Erfüllung gefährden könnte. Diese „Hilfskonstruktion“ ist jedoch aufgrund § 14 Abs 5 DSG 2000 nicht mehr erforderlich, da Protokoll- und Dokumentationsdaten mindestens drei Jahre aufbewahrt werden müssen. Für den Ersatz des ideellen Schadens hat sich nun mehr die jene schadenersatzrechtliche Lehre durchgesetzt,⁴⁵⁹ dass dieser nur bei grober Fahrlässigkeit und Vorsatz zusteht.

⁴⁵⁵ Duschaneck, DSG, 52

⁴⁵⁶ OGH 10.7.1986, 6 Ob 12/85, EDVuR 1986 H.3, 27

⁴⁵⁷ OGH 05.05.1988, 6 Ob 9/88

⁴⁵⁸ Ähnlich bereits OGH SZ 59/123= JBl 1986, 663=RdW 1986, 307 wo jedoch der Klage stattgegeben wurde, weil nicht behauptet wurde, dass die begehrten Angaben nicht mehr rekonstruiert werden können

⁴⁵⁹ F. Bydlinski, Der Ersatz ideellen Schadens als sachliches und methodisches Problem, JBl 1965, 173, 237 ff, Koziol, Haftpflichtrecht², I 228 ff, Koziol/Welser, Grundriss I 424; Mayrhofer, Schuldrecht Allgemeiner Teil (1986) 323 f

In zwei E des OGH⁴⁶⁰ wurde das Auskunftsbegehren eines Bankkunden über die Verarbeitung von Daten betreffend Zinssätze und sonstige Konditionen mit Berufung auf das Schikaneverbot⁴⁶¹ als unberechtigt qualifiziert da der Betroffene von diesen Daten bereits durch ihm zugestellten Kontoauszüge, Wertpapierabrechnungen und Eintragungen ins Spargbuch Kenntnis erlangt hatte. Er hätte darin glaubhaft machen müssen, dass diese Daten beim Auftraggeber (der Bank) irrtümlich oder missbräuchlich vorhanden sind. Der OGH meint dazu *„Als bürgerrechtlicher Anspruch unterliegt das Auskunftsrecht des § 25 DSGVO (1978) allerdings dem Schikaneverbot...“*

Daraus ergibt sich die Einschränkung, dass wenn die Informationen eine Wiederholung bereits erteilter Informationen darstellen weil der Betroffene aufgrund rechtsgeschäftlicher Beziehung diese bereits erhalten hat, so ist eine datenschutzrechtliche Auskunft als Grundlage seiner Rechtsverfolgung nicht mehr notwendig/erforderlich weil es überflüssig wäre, ihm Daten nochmals nach dem Datenschutzgesetz zu beauskunften, über die er ohnehin bereits aufgrund einer Mitteilung in anderem Zusammenhang verfügt.

Zu beachten ist jedoch, dass wenn der Betroffene einen Bedarf an zusätzlicher Information glaubhaft machen kann, insbesondere bei vermuteter Unrichtigkeit oder irrtümlicher oder gar missbräuchlicher Verwendung, der datenschutzrechtliche Auskunftsanspruch davon unberührt bleibt.⁴⁶²

Noch immer nicht endgültig geklärt, ob dies auch auf die schuldhafte Verletzung der Auskunftspflicht zutrifft. Das Recht auf Auskunft dient zwar nicht unmittelbar dem Geheimhaltungsinteresse des Betroffenen doch wird es für ihn die einzige Möglichkeit sein, unzulässige Eingriffe in sein Persönlichkeitsrecht festzustellen und dadurch (weitere) Ansprüche nach dem Datenschutzgesetz geltend zu machen.⁴⁶³ Es scheint daher sachgerecht, dass die schuldhafte Verletzung der Auskunftspflicht an die selben Rechtsfolgen anknüpft wie bei der Verletzung von sonstigen Persönlichkeitsrechten wie Wahrung der Geheimsphäre und Achtung des Privatlebens weil ansonsten es der Auskunftspflichtige in der Hand hätte, durch Verweigerung der Auskunft die Verfolgung anderer Ansprüche aus rechtswidrigem Verhalten nach dem Datenschutzgesetz zu vereiteln.⁴⁶⁴

⁴⁶⁰ OGH 6 Ob 24/90 bzw. 25/90 vom 13. 12.1990 in EDVuR 1991/I, 71 m. Anm. *Duschanek*

⁴⁶¹ § 1295 Abs 2 lautet: *Auch wer in einer gegen die guten Sitten verstößenden Weise absichtlich Schaden zufügt, ist dafür verantwortlich, jedoch falls dies in Ausübung eines Rechtes geschah, nur dann, wenn die Ausübung des Rechtes offenbar den Zweck hatte, den anderen zu schädigen*

⁴⁶² *Wittmann*, Datenschutzrecht im Unternehmen, 114ff

⁴⁶³ Siehe auch OGH SZ 59/123 = JBl 1986, 663 = RdW 1986, 307 = EDVuR 1986/3, 27

⁴⁶⁴ In diesem Sinne *Schauer*, Die Grenzen des datenschutzrechtlichen Auskunftsbegehrens, RdW 1989/4, 121 ff

Sollte sich der Auftraggeber eines Dienstleisters bedienen, so ist dieser nach § 11 Abs 1 Z 4 DSG 2000 verpflichtet (soweit dies nach der Art der Dienstleistung in Frage kommt), im Einvernehmen mit dem Auftraggeber die Voraussetzungen für die Erfüllung der Auskunftspflicht (sowie Richtigstellungs- und Löschungspflicht) zu schaffen. Der Auftraggeber kann den Dienstleister auch zur Erledigung von Auskunftsansprüchen ermächtigen, bleibt aber im Außenverhältnis dem Betroffenen gegenüber bei der Erfüllung der Auskunftspflicht verantwortlich.

Umfang und Inhalt des Auskunftsrechts beschränkt sich nicht nur auf die Art der gespeicherten Daten sondern hat der Betroffene auch ein Recht den konkreten Inhalt dieser Daten zu erfahren⁴⁶⁵ weil erst ab Kenntnis des konkreten Dateninhalts kann der Betroffene beurteilen ob ihm allenfalls ein Richtigstellungs-, Löschungs- oder Unterlassungsanspruch zusteht. Dh zB nicht nur „persönliche Daten“ sondern Vor- und Zuname, Adresse, (Geburtsdatum - falls vorhanden), usw.

Der Betroffene kann auch Auskunft über die Herkunft der Daten sowie über Empfänger (-kreise) bei Übermittlung verlangen. Unter Herkunft der Daten ist jedoch nicht die gesamte Information aller Vormänner gemeint. Es genügt die Benennung des letzten Vormanns.⁴⁶⁶

Gerade Bonitätsinformationen über einen Unternehmer oder auch über eine Privatperson sind für das Zustandekommen von Geschäfts- oder Vertragsabschlüssen heutzutage sehr entscheidend. Daher besteht ein evidentes Interesse, die Empfänger dieser Auskünfte konkret benannt zu erhalten um einerseits die Rechtmäßigkeit der Übermittlung nachprüfen zu können und um ein entsprechendes Verhalten der Empfänger vorhersehen oder nach verfolgen zu können. Stellt der Betroffene nämlich bei der Prüfung der ihm erteilten Auskunft fest, dass unrichtige Daten betreffend seine Bonität übermittelt wurden, so muss er sich nicht darauf verlassen, dass der Auftraggeber seiner Pflicht gemäß § 27 Abs 8 DSG 2000 (Verständigung der Übermittlungsempfänger von einer durchgeführten Richtigstellung) nachkommen wird. Der Betroffene hat vielmehr ein überwiegendes berechtigtes Interesse daran, alle beim Auftraggeber vorhandenen Daten der Übermittlungsempfänger zu erhalten, die er benötigt, um diese nötigenfalls selbst ansprechen zu können. Die Auskunft müsse daher grundsätzlich so konkret erfolgen, dass der Betroffene sein Löschungs- und Richtigstellungsrecht sowohl gegenüber der Quelle (Herkunft) als auch gegenüber

⁴⁶⁵ OGH 10.7.1986, 6 Ob 12/85, EDVuR 1986 H.3, 27 [FN 163]

⁴⁶⁶ Wittmann, Datenschutzrecht im Unternehmen, 116; OGH 28.10.1999; OGH 3Ob132/99d, ecolx 2000, 578

Übermittlungsempfänger geltend machen könne. Das in § 26 Abs 1 DSG 2000 verankerte Auskunftsrecht umfasse sowohl die Herkunft als auch die Empfänger(-kreise) und das Interesse des Betroffenen an der Auskunft über diese Daten sei nicht weiter begründungsbedürftig. Dieses Auskunftsrecht ist jedoch nicht schrankenlos sondern habe eine Interessensabwägung zwischen den Auskunftsinteressen des Betroffenen und den Geheimhaltungsinteressen des Auftraggebers oder eines Dritten zu erfolgen. Geheimhaltungsinteressen sind konkret dh auf das jeweils bekannt zu gebende Datum geltend zu machen. Für allgemeine Aussagen wie Geschäftsgeheimnisse, Geheimhaltungsinteressen Dritter besteht hiezu kein Platz. Hinsichtlich der alternativen Formulierung „Empfänger oder Empfängerkreise“ (in § 26 Abs 1 DSG 2000) wird auf Art 13 der Datenschutz RL und deren Erwägungsgrund 41, wonach der Schutz des Geschäftsgeheimnisses nicht dazu führen dürfe, dem Betroffenen jegliche Auskunft zu verweigern. Dem wird durch die Interessenabwägung Rechnung getragen.⁴⁶⁷

Wer sein Auskunftsrecht rechtmäßig ausübt darf nicht durch „indirekte/fiktive Kosten“ wie zB wirtschaftlich oder in anderer Weise, benachteiligt werden. Betroffene welche häufig von ihrem Auskunftsrecht Gebrauch machen, dürfen nicht in ihrer Bonität/Kreditwürdigkeit herabgestuft werden. Aus der Tatsache, dass verstärkt Bonitätsauskünfte eingeholt werden, schließen manche Auskunftseien, der Betroffene wolle sich offenbar durch eine Großanschaffung verschulden. Dieser Schluss und das damit implizierte Verhalten ist eindeutig rechtswidrig.⁴⁶⁸

Auch nach erfolgter Löschung von Daten aufgrund eines Urteils des Landesgerichts gemäß § 27 DSG 2000 steht dem Betroffenen beliebig oft das Recht auf Auskunft iSd § 26 Abs 6 DSG 2000 zu sofern es sich nicht um schikanöse Rechtsausübung handelt. Denn nur gerade dadurch ist sichergestellt, dass der Betroffene sich laufend Einblick in die aktuelle Datenverarbeitung des Auftraggebers verschaffen kann um in weiterer Folge seine Rechte wahren zu können. Das Argument ein Auskunftsbegehren nach erfolgter Löschung könne nicht gefordert werden wurde von der DSK nicht anerkannt. In diesem Fall hätte somit eine „Negativauskunft“ erteilt werden müssen.

Auch der zuvor gemachte Hinweis an den Auskunftswerber, dass sämtliche (weitere) Kommunikation nur mit bzw. an seinen bestellten (Rechts-)vertreter zu erfolgen hätte,

⁴⁶⁷ GZ K121.290/0015 – DSK/2007 vom 3. Oktober 2007; VwGH vom 19.12.2006, Zl. 2005/06/0111 (abgewiesene Beschwerde gg. den Bescheid der DSK GZ K120.981/0002-DSK/2005 vom 15. Februar 2005)

⁴⁶⁸ Duhr in Rossmagel, Handbuch Datenschutzrecht, Kap. 7.5, RNR 86

mindert in keinster Weise die Wirksamkeit der Zustellung direkt an den Auskunftspflichtigen.⁴⁶⁹

Ein juristisch heikler aber immer häufiger auftretender Sachverhalt betrifft die Verarbeitung und Bewertung von personenbezogenen Daten im Rahmen eines „Scoring Systems“. Dabei werden die persönlichen Daten des Kunden aufgrund von empirischen Erhebungen über die Zahlungsausfallwahrscheinlichkeit, einem Punktesystem unterzogen an dessen Ende eine Kreditentscheidung zu Gunsten oder zu Lasten des Kunden steht. Eine vollautomatische Entscheidungstechnik ohne menschlichen Eingriff ist iSd § 39 DSG 2000 jedoch verboten.

Ein (Telekom-)Unternehmen bediente sich zur Errechnung des Scorewertes ihrer Kunden einer Kreditauskunftei welche einerseits die Bonitätsdaten zur Verfügung stellt andererseits auch das „Grundgerüst“ des Scoring Verfahrens erstellt und dieses auch auf Verlangen des Kunden „customized“ und fortwährende Verbesserungen und Änderungen durchführt. Ab dem Zeitpunkt wo Kundendaten in das Scoring System eingespeist werden, wird der Eigentümer des Systems zum datenschutzrechtlichen Auftraggeber. Solange das Unternehmen das System vorgibt, nach dem die Berechnung zu erfolgen hat, ist sie Auftraggeber und verantwortlich für die von ihr in Auftrag gegebene Bonitätsprüfung durch die Kreditauskunftei. Zu diesen Pflichten gehört sowohl die rechtzeitige Löschung von Daten zu veranlassen als auch der Auskunftspflicht gemäß § 26 DSG 2000 nachzukommen.

Der Einwand des (Telekom-)Unternehmens sie dürfe aufgrund § 97 Abs 2 TKG 2003 gar keine Stammdaten iSd § 92 Abs 3 Z 3 lit f TKG 2003 (worunter auch die Bonität von [möglichen] Kunden fällt) speichern, wird insoweit nicht gefolgt, da sie als Auftraggeber auch für die Daten der Kreditauskunftei als Dienstleister verantwortlich ist andererseits das Auskunftsrecht gerade auch nicht rechtmäßig verarbeitete Daten einbezieht. Dies ergibt sich auch § 26 Abs 7 DSG 2000 dass ab Kenntnisnahme des Auskunftsbegehren eine Löschungssperre auferlegt, die den Auftraggeber bei Strafe (§ 52 Abs 1 Z 4 DSG 2000) hindert, sowohl rechtmäßige als auch unrechtmäßig verarbeitete Daten, einer Auskunft durch Löschung zu entgehen. Dem (Telekom-)Unternehmen wurden sodann durch einen Leistungsbescheid iSd § 59 Abs 2 AVG der DSK welcher auch zwangsweise vollstreckt werden kann, aufgetragen innerhalb von zwei Wochen sämtliche betreffende Bonitätsdaten und Scoring Werte dem Betroffenen mitzuteilen oder zu begründen, warum die Auskunft nicht oder nicht vollständig erteilt wird. Dieser Bescheid der DSK wird soeben beim VwGH

⁴⁶⁹ GZ K121.356/0005-DSK/2008 vom 30.Mai 2008

angefochten⁴⁷⁰. Auf das Ergebnis kann man gespannt sein. Wenn die zuständigen Richter mit dem Ablauf einer Bonitätsprüfung bei einem Telekomunternehmen firm sind, dann gibt es jedoch an der Entscheidung der DSK nichts zu rütteln da sie den Sachverhalt sowie die Geschäfts- und Kompetenzaufteilung ganz richtig erkannt hat.⁴⁷¹

Da es sich beim Thema Datenschutz im privaten Bereich, vor allem auch Bonitätsinformationen betreffend, um eine sehr sensible (wenn auch nicht im juristischen Sinn als „sensible Daten“ klassifiziert) handelt, tut jeder Auftraggeber gut daran bzw. ist er sogar verpflichtet, sämtliche Informationen an den Betroffenen zu übermitteln. Auch wenn in diesem Fall keine Daten bestehen, keine Übermittlung an Empfänger statt gefunden hat, so ist dies dem Auskunftswerber mitzuteilen andernfalls sich dieser in seinem Recht auf Auskunft verletzt sieht. Sollte ein Auftraggeber über mehrere unterschiedliche Bonitätsdatenbanken verfügen und er ein allgemeines Auskunftsbegehren erhalten, so ist über alle ihn betreffenden Daten in allen Datenbanken (und nicht nur über eine spezifische) Auskunft darüber zu geben bzw. zu begründen warum diesbezüglich keine Informationen bekannt geben werden (können). (§ 26 Abs 4 DSG 2000)⁴⁷²

Die Auskunft bezieht sich nach § 26 Abs 6 DSG 2000 immer auf den „aktuellen Datenbestand“. Das Argument des Auskunftspflichtigen Herkunfts- und Übermittlungsempfänger entsprechen nicht diesem Tatbestand folgte die DSK genau so wenig wie ein verlangtes zusätzliches Entgelt zur Abgeltung des (manuellen) Mehraufwandes. Aus dem AB zu § 26 DSG 2000 ist zu entnehmen, dass eine Auskunft über „Protokolldaten“ aus der technischen Abwicklung der Datenverarbeitung unterbleiben kann.⁴⁷³

Aus den Erläuterungen zur RV des DSG 2000 zu § 26 Abs 6 DSG 2000 geht hervor, dass damit die technische Frage beantwortet werden soll ob die Auffindung einen besonderen Aufwand erfordert. Dabei wird sogar noch auf die 1986 novellierte Vorläuferbestimmung des § 11 DSG und dessen Materialien Bezug genommen wo es heißt „Der aktuelle Datenbestand im Sinne dieser Regelung ist entweder der im Direktzugriff stehende oder – mangels eines solchen – der letztgültige Datenbestand.“ Eine Überprüfung vor Ort hat auch ergeben, dass Übermittlungsempfänger zum aktuellen Datenbestand gehören und auf „Knopfdruck“ abrufbar sind und daher eine Zurückhaltung der Auskunft bis zur Begleichung eines

⁴⁷⁰ VwGH ZI 2008/17/0097

⁴⁷¹ GZ K121.339/0007-DSK/2008

⁴⁷² GZ K121.326/0002-DSK/2008 vom 18.Jänner 2008

⁴⁷³ *Duschanek*, § 1 DSG in *Korinek/Holoubek* (Hrsg), Österr BVfR – GR III, Rz 80

Kostenersatzes den Betroffenen in seinem Auskunftsrecht verletzt hat. Es wurde darauf hin ein Leistungsbescheid iSd § 59 Abs 2 AVG mit einer zweiwöchigen Frist zur Bekanntgabe erlassen.⁴⁷⁴

Unter § 26 Abs 4 DSG 2000 unter bestimmten Voraussetzungen vorgesehene schriftlich begründete Ablehnung der Auskunft ist – auch im öffentlichen Bereich – als bloße Mitteilung ohne Bescheidcharakter zu verstehen.⁴⁷⁵ (zu beachten sind die Ausnahmen bezüglich Standard- und Musterverordnung iSv § 14 Abs 3 DSG 2000)

Kurz zusammengefasst hat die Auskunft folgende Informationen in allgemein verständlicher Form zu enthalten:

- die verarbeiteten Daten
- die verfügbaren Informationen über ihre Herkunft
- allfällige Empfänger oder Empfängerkreise bei Übermittlungen
- den Zweck der Datenverwendung
- die Rechtsgrundlagen
- (- Name und Adresse von Dienstleistern auf Verlangen des Auskunftswerbers)

Beispiel:⁴⁷⁶

⁴⁷⁴ GZ K121.335/0005-DSK/2008 vom 29. Februar 2008; K121.334/0005-DSK/2008 vom 28. Februar 2008

⁴⁷⁵ Dohr-Pollirer-Weiss, Datenschutzgesetz, 67 u. 69 mit Hinweis auf DSG 14.12.1984, ZfVB 1987/2/3; Duschanek, DSG 2000, 102, Duschanek/Rosenmayr-Klemenz, 102

⁴⁷⁶ Nach Knyrim, Datenschutzrecht, 224

Sehr geehrte.....

Zu Ihrem Auskunftersuchen nach § 26 DSG 2000 teilen wir wie folgt mit:

- 1. Wir verarbeiten folgende Daten von Ihnen: (Aufzählung sämtlicher Daten die über den Betroffenen gespeichert sind.*
- 2. Diese Daten haben wir (zB aufgrund ihrer eigenen Angaben/aus dem Telefonbuch/Adressverlag XY/Auskunftei XY) erhalten.*
- 3. Wir haben diese Daten (zB an niemanden/an folgendeübermittelt)*
- 4. Wir verarbeiten Ihre Daten zum Zweck der (zB Durchführung ihrer Bestellung/Bewerbung unserer Produkte/Vertragserfüllung/Bonitätsprüfung...)*
- 5. Die Rechtsgrundlage für die Verarbeitung Ihrer Daten durch uns ist (zB unsere Gewerbeberechtigung nach §§ 151 oder 152.....)*

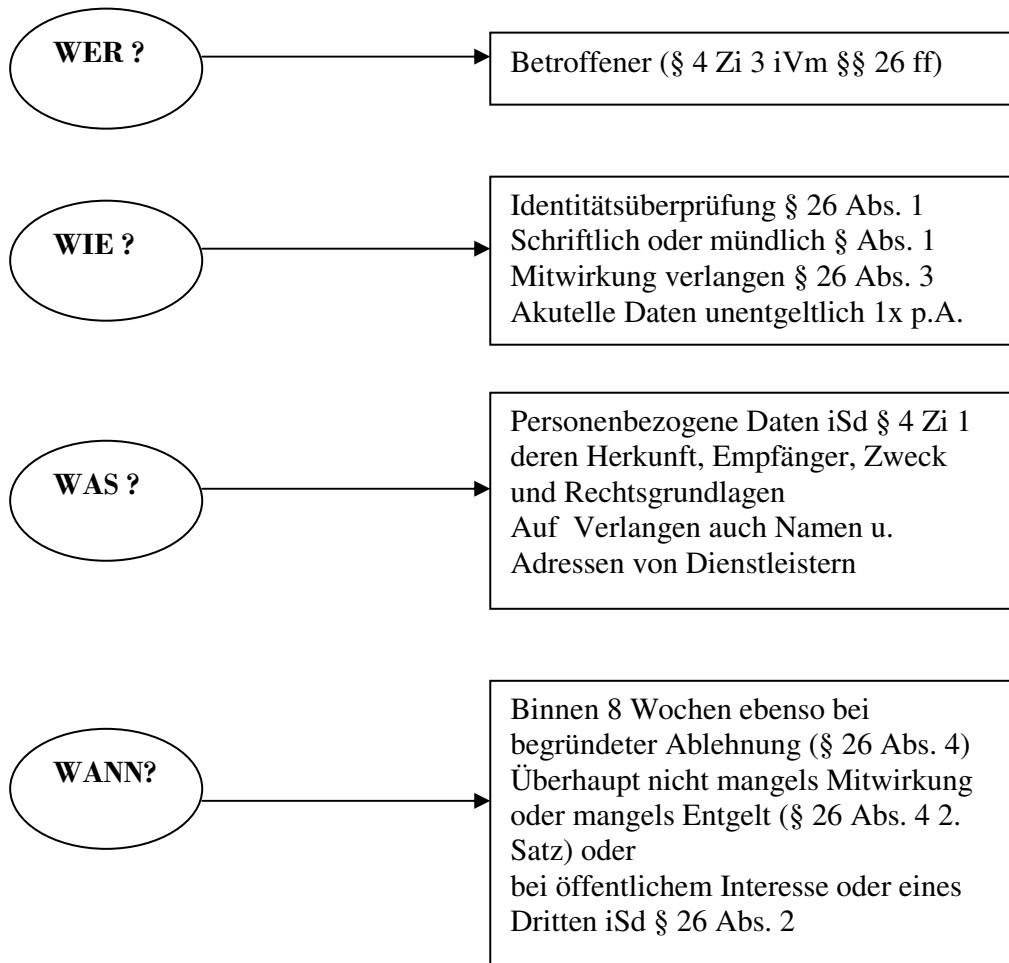
Aber auch in der „umgekehrten,, Richtung gibt es ein Recht auf Auskunft. In dem Fall das jemand bei einer Kreditunternehmung, Investmentgesellschaft oder ähnliches arbeitet und von dieser einen Privatkredit beantragt, hat der Arbeitgeber iSv § 28 Abs 1 Z 6 iVm Abs 2 Z 1 BWG zu prüfen ob und wie hoch die Kreditverpflichtungen des Angestellten sind und das im Gesetz genannte Viertel des Jahresbezuges übersteigt. Der Arbeitgeber hat sich jedoch zuerst an den Arbeitnehmer selbst zu wenden und kann von diesem eine entsprechende Auskunft verlangen. Der Arbeitnehmer ist aufgrund der aus

§ 1153 ABGB ergebenden Treuepflicht zur wahrheitsgemäßen Beantwortung verpflichtet. Eine unwahre Angabe könnte als Entlassungsgrund gemäß § 27 Z 1 AngG wegen Vertrauenswürdigkeit ausgelegt werden. Obwohl der VfGH bekanntlich ja entschied, dass das verfassungsrechtlich gewährleistete Recht auf Datenschutz auch nicht automationsunterstützt verarbeiteter personenbezogener Daten umfasst,⁴⁷⁷ wird auch eine Anfrage beim KSV über den eigenen Angestellten iSv § 8 Abs 1 Z 4 bei überwiegendem Interesse des Auftraggebers oder gar bei Zustimmung iSd Z 2 gerechtfertigt sein.

Somit gibt sich kurz zusammengefasst folgendes Bild („check box“)⁴⁷⁸

⁴⁷⁷ VfGH 12.10.1989, G 237 – 241/88, V 209 – 212/88; infas 1990 H 6, 4

⁴⁷⁸ Nach Weiss/Pollirer, Datenschutz in der Wirtschaft II, RWZ 1993/8,251



14.2. Recht auf Richtigstellung oder Löschung

Der Grundsatz des § 6 Abs 1 Z 4 („Verwendung von Daten wenn sie „im Hinblick auf den Verwendungszweck sachlich richtig“ und auf dem „neuesten Stand sind“) wird durch § 27 Abs 1 DSG 2000 präzisiert. Unvollständige Daten sind dann berichtigungspflichtig, wenn sich aus der Unvollständigkeit in Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. „Löschen“ im Sinne des § 27 DSG 2000 bedeutet das Unkenntlichmachen von Daten ohne die Möglichkeit ihrer Rekonstruktion, dh es muss programmtechnisch oder wenigstens organisatorisch Vorsorge getroffen werden, dass gelöschte Daten nicht wieder benützt werden können.⁴⁷⁹ Davon zu unterscheiden ist das Vernichten des Datenträgers sowie das „logische Löschen“. Bei letzterem wird nur die Verknüpfung zu einem Index (typischerweise reversibel) aufgehoben, weshalb dieser Vorgang zutreffend nicht als Löschen sondern als Sperren zu qualifizieren ist.⁴⁸⁰

Der Auftraggeber ist zur Richtigstellung oder Löschung ermittelter oder verarbeiteter Daten nicht durch jeden Antrag eines Betroffenen, sondern nur durch begründeten Antrag verpflichtet. Eine bloße Behauptung der Unrichtigkeit von Daten vermag somit eine Richtigstellungs- oder Löschungspflicht nicht automatisch zu entfalten.⁴⁸¹ Werturteile können zwar objektiv verfehlt sein, ohne als tatsächlich erfolgt Meinungsäußerung des Urteilenden unrichtig zu sein.⁴⁸²

Jedoch ist der Auftraggeber selbständig dazu verpflichtet, unrichtige oder unzulässig verwendete Daten richtig zu stellen oder zu löschen wenn ihm dies aus eigenem Verhalten bekannt wurde.⁴⁸³ (ausgenommen sind Daten die ausschließlich aufgrund von Angaben des Betroffenen ermittelt wurden) So werden die Adressen von Personen in einer Kreditevidenz/Kreditauskunft nur soweit von Bedeutung sein, als die einmeldenden Unternehmen selbst ein großes Interesse an der Aktualität dieses Datums haben und bei bekannt werden, eine Änderung vornehmen bzw. weitermelden.

⁴⁷⁹ ÖZW 1979/1,14

⁴⁸⁰ Drobosch/Grosinger, DSG, 122ff; aA Dohr/Pollirer/Weiss, DSG², § 4 Anm 9

⁴⁸¹ GZ 120.607/10-DSK/99 vom 2. Juli 1999; aA Duschaneck, § 1 DSG in Korinek/Holoubek (Hrsg), Österr BVfR – GR III, Rz 82 der ein Richtigstellungsbegehren nicht auf eine bestimmte Interessenslage stützt. Die in § 27 Abs 1 Z 2 DSG 2000 verlangte Begründung ist schon mit der Behauptung der Unrichtigkeit ausreichend.

⁴⁸² Zur Unrichtigkeit bzw Richtigstellung personenbezogener Daten *Mallmann* in *Simitis*, § 20 BDSG, Rz 10ff und § 35 BDSG, Rz 7; *Dammann/Simitis*, EG DS-RL, 197

⁴⁸³ § 27 Abs 1 Z 1 DSG 2000

Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf einer Entscheidung des zuständigen Gerichts oder der DSK gelöscht werden.⁴⁸⁴ (§ 27 Abs 3 DSG 2000). Lässt sich auch in einem gerichtlichen oder behördlichen Beweisverfahren die Richtigkeit oder Unrichtigkeit nicht bestätigen, so wird das Gericht oder die DSK eine Interessensabwägung iSd § 1 DSG 2000 durchführen und über die Aufrechterhaltung des Bestreitungsvermerk entscheiden.

Die DSK hat weiters festgehalten, dass eine vom Betroffenen verlangte „Auskunftssperre“ rein rechtlich gesehen, ein „Minus“ zum gesetzlich eingeräumten Lösungsanspruch darstellt, und dieser ihm daher ebenso zu steht. Eine Verarbeitung mit dem beigefügten Vermerk „Die angefragte Firma wünscht, dass keine Auskünfte über sie erteilt werden. Daraus kann jedoch nicht unmittelbar auf eine verschlechterte Bonitätslage geschlossen werden“ stellt jedoch eine Aushöhlung des auf volle Löschung (oder auf Sperre) gerichteten Widerspruchrechts dar und ist daher rechtswidrig und zu entfernen.⁴⁸⁵

Natürlich gilt es die siebenjährige Aufbewahrungspflicht nach § 212 UGB und im Steuerrecht nach § 132 BAO zu beachten welche aber wiederum nur eine Ausnahme vom Grundrecht auf Datenschutz iSd § 1 Abs 2 DSG 2000 (Eingriff staatlicher Behörden) darstellt. Daher besteht keine generelle Datenspeicherungspflicht für Unternehmen, sondern eigentlich ein generelles Verbot zur Datenverarbeitung, dass nur aus bestimmten Gründen (Zustimmung, Notwendigkeit zur Vertragserfüllung etc) oder auf Grund von gesetzlichen Normen (Aufbewahrungspflichten nach Handels- und Steuerrecht) durchbrochen wird. Diese Fristen sind Maximalfristen für eine Datenaufbewahrung und nach Ablauf dieser Fristen müssen die Daten sofort gelöscht werden, soweit nicht ein anderer Grund für ihre Aufbewahrung vorliegt.⁴⁸⁶ Nicht ausdrücklich geregelt ist das Problem der Dauer der Auskunftspflicht in § 26 DSG 2000. Über gelöschte Daten kann natürlich keine Auskunft gegeben werden und eine Verjährung dieser aus dem Persönlichkeitsrecht auf Datenschutz herrührenden Rechtes kommt nach § 1459 ABGB nicht in Betracht.⁴⁸⁷

Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, wenn der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zulässt. Die

⁴⁸⁴ Dohr/Pollirer/Weihs, DSG, Anm 21 zu § 27 DSG; Knyrim, Datenschutzrecht, 227

⁴⁸⁵ GZ K211.593/0011-DSK/2005 vom 29. November 2005

⁴⁸⁶ Knyrim, Datenschutzrecht, 9

⁴⁸⁷ Koziol/Welser, Grundriss I

notwendigen Richtigstellungen sind in diesem Fall durch entsprechende Zusatzvermerke durchzuführen.

Eine nachträgliche Änderung wird insbesondere dann nicht zugelassen sein, wenn die Datenanwendung dazu dient, den tatsächlichen Ablauf festzuhalten. (zB Entstehung einer (Groß-)insolvenz oder einer Krankengeschichte)

*Stadler*⁴⁸⁸ sieht in der Richtigstellung von Daten welche auf Antrag des Betroffenen durchgeführt wurden, ein zivilrechtliches Anerkenntnis. Hier ist jedoch zu unterscheiden.

Das Anerkenntnis ist in der österreichischen Rechtsordnung nicht besonders gesetzlich geregelt (ausgenommen in familienrechtlichen Abstammungssachen) und wird prinzipiell als Sonderform des Vergleichs behandelt. Vom Vergleich (§ 1380 ABGB) unterscheidet es sich dadurch, dass ein Vertragspartner nicht nachgibt, sondern der andere das zuerst bezweifelte Recht in vollem Umfang zugesteht. Ein so genanntes „*konstitutives Anerkenntnis*“ kommt dann zustande, wenn ein Vertragspartner eines strittigen Rechtsverhältnisses ein Recht ernstlich behauptet und der andere Vertragspartner die Unsicherheit der Rechtslage mit seinem Anerkenntnis beseitigt.⁴⁸⁹ Ein solcher Feststellungsantrag schafft unabhängig vom Bestehen des behaupteten Rechtes eine neue selbständige Verpflichtung.

Lehre und Praxis kennt auch noch das „*deklaratorische (oder auch unechte) Anerkenntnis*“ welches bloß eine Wissenserklärung darstellt. Der Anerkennende will keine Rechtsfolgen herbeiführen, sondern gibt nur bekannt, dass das Rechts des Gläubigers seines Wissen nach besteht. Dieses Anerkenntnis schafft keinen neuen Verpflichtungsgrund, sondern bildet im Rechtsstreit höchstens ein Beweismittel.

Daraus lässt sich erkennen, dass die Richtigstellung von Daten keinesfalls immer als konstitutives Anerkenntnis angesehen werden kann sondern an den Umständen des Einzelfalls zu lösen ist.⁴⁹⁰

Mit der ZVN 2004 wurden die §§ 83 bis 85 GOG eingeführt um die betreffenden Gesetze an die Vorgaben des DSG 2000 anzupassen und einen Rechtsbehelf gegen die Verletzung des Grundrechts auf Geheimhaltung durch Organe der Gerichtsbarkeit zu schaffen und um eine Lücke zu schließen weil Akte der Gerichtsbarkeit vom Rechtsschutzsystem des Datenschutzes ausgenommen waren und keine Zuständigkeit der DSK bestand. Gemäß § 84 GOG hat das für die Eintragung von Daten zuständige Gericht (Auftraggeber iSd § 4 Z 4 DSG 2000) über

⁴⁸⁸ *Stadler*, ÖZW 1979

⁴⁸⁹ OGH 29.1.1974, JBl 1975, 206

⁴⁹⁰ *Hanreich* in Datenschutz in der Wirtschaft, Zivilrechtliche Probleme des DSG, 91ff; *Koziol/Welser*, Grundriss I; zur Auslegung von Erklärungen von Anerkenntnissen siehe OGH 1.7.1976, JBl 1977, 486ff welcher nach den Grundsätzen des redlichen Verkehrs zu erfolgen hat

den Löschantrag in bürgerlichen Rechtssachen in Verfahren außer Streitsachen zu entscheiden.

Ein von einem Betroffenen gestellter Antrag „auf Löschung personenbezogener Daten im Sinne des § 73a Exekutionsordnung (EO)“⁴⁹¹ aus dem „*Exekutionskataster*“ wurde durch das Erstgericht abgewiesen. Das gegenständliche Exekutionsverfahren sei bereits infolge Zahlung der verpflichteten Partei eingestellt worden. Der OGH⁴⁹² entschied, nach einer Änderung der Rechtslage aufgrund eines Erkenntnisses des VfGH⁴⁹³, dass die elektronische Einsicht in Geschäftsbehalte des Exekutionsverfahrens bei einer nachträglichen Änderung des Aussagewerts der Daten zu beschränken sei. Bei einer Einstellung des Exekutionsverfahrens wegen Befriedigung des betreibenden Gläubigers sei dieser Umstand (Status) in der uneingeschränkten Auskunft nur zu ergänzen. Eine Löschung der Daten komme nicht in Betracht.

⁴⁹¹ § 73a lautet: (1) Der Bundesminister für Justiz hat nach Maßgabe der technischen Möglichkeiten sowie unter Bedachtnahme auf eine einfache und sparsame Verwaltung und eine Sicherung vor Missbrauch die Geschäftsbehalte des Exekutionsverfahrens, insbesondere die Namensverzeichnisse, die Register über Pfändungen und die Listen der Vermögensverzeichnisse, zu bestimmen, in die Rechtsanwälte, Notare und Körperschaften des öffentlichen Rechts mittels automationsunterstützter Datenübermittlung Einsicht nehmen dürfen, wenn sie die auf diese Weise erlangten Daten zur Einleitung eines Rechtsstreites oder einer Exekution, zur Geltendmachung von Einwendungen gegen eine bereits eingeleitete Exekution oder sonst zur Führung eines gerichtlichen Verfahrens benötigen.

(2) Die Einsicht ist nach Maßgabe der technischen Möglichkeiten für den Sprengel eines Bezirksgerichts oder eines Landesgerichts oder bundesweit zu ermöglichen.

(3) Die nähere Vorgangsweise bei dieser elektronischen Einsicht ist durch Verordnung des Bundesministers für Justiz zu regeln.

⁴⁹² OGH 25.4.2007, 3 Ob 31/07s, JusGuide 2007/26/4856 (OGH)

⁴⁹³ VfGH vom 12. 12. 2002, G 194/02, V 45/02

14.3. Widerspruchsrecht

Hiemit wird dem Betroffenen in § 28 DSG 2000 (aufgrund der Vorgabe von Art 14 der DS-RL) die Möglichkeit geboten gegen die Verwendung seiner Daten sowohl beim öffentlichen als auch privaten Auftraggeber zu urteilen, und diesem die Verwendung seiner Daten bei überwiegend schutzwürdiger Geheimhaltungsinteressen zu verwehren. Das Widerspruchsrecht iSd § 28 DSG 2000 ist vom Recht des Kunden, eine bereits erteilte Zustimmung zur Datenverwendung zu widerrufen, zu unterscheiden. Das Widerspruchsrecht kommt daher einem Betroffenen demnach nur dann zu, wenn er aus seiner besonderen Situation heraus ein erhöhtes Interesse an der Geheimhaltung der verarbeiteten Daten geltend machen kann, welches bei einer Durchschnittsbetrachtung von anderen Betroffenen nicht vorherrscht.⁴⁹⁴

Die Daten sind sodann innerhalb von acht Wochen zu löschen. Die Rechtsfolgen eines erfolgreichen Widerspruchs manifestieren sich darin, dass die betroffenen Daten nicht erhoben, verarbeitet oder genutzt werden dürfen. Ist eine Verarbeitung jedoch bereits erfolgt, so wird die Speicherung „ex-nunc“ (arg. „nicht mehr“) unzulässig und bewirkt eine Verpflichtung zu Löschung der Daten. Hat der Betroffene nur Widerspruch gegen Übermittlung oder Nutzung erhoben und ist damit durchgedrungen, so ist dies zukünftig unzulässig.⁴⁹⁵ Aber da eine genauere Definition auch in den Erläuterungen zum DSG 2000 fehlt und auch in der Datenschutz RL keine Beispiele angeführt werden⁴⁹⁶, liegt es wohl einerseits in der Hand des Betroffenen seine Gründe möglichst glaubhaft zu machen und andererseits beim Auftraggeber diese zu beachten oder auch nicht. Er muss daher aus seiner besonderen Situation darlegen, worin sich seine Situation von derjenigen anderer unterscheidet und warum im konkreten Einzelfall eine an sich rechtmäßige Verarbeitung gleichwohl eine Abstandnahme von der Verarbeitung begründen kann.⁴⁹⁷ Ein Widerspruch muss nicht ausdrücklich als solcher bezeichnet werden sondern kann auch konkludent zum Ausdruck gebracht werden.

Dieses Widerspruchsrecht besteht jedoch nicht, wenn die Verwendung der Daten gesetzlich vorgesehen ist. Der Unterschied zu einer Beschwerde bzw. Klage wegen unzulässiger

⁴⁹⁴ Dohr-Pollirer-Weiss, DSG², Anm 4 zu § 28

⁴⁹⁵ Gola, DuD 2001, 278

⁴⁹⁶ Duschaneck, Neuerungen und offene Fragen im DSG 2000, ZfV 2000/1303, 534; zu Auslegungsproblemen auch Dammann/Simtis, EU DS-RL, 213f; Ehmann/Helfrich, EG DS-RL, Art 14, 211f

⁴⁹⁷ Der Betroffene muss daher *eigene* personenbezogene Daten dem Auftraggeber mitteilen, wenn er sein Widerspruchsrecht geltend machen will. Dabei wird man jedoch nicht zu große Anforderungen an ihn stellen dürfen obwohl Duhr/Naujok/Danker/Seiffert, DuD 2003, 1, 19 von einer „präzisen und umfangreichen“ Darlegung sprechen; Ehmann/Helfrich, EG DS-RL, Art 14, Rn 17

Verarbeitung nach §§ 31 und 32 DSG 2000 liegt alleine darin, dass die Ausübung des Widerspruchsrechts keinen Einfluss auf die rechtliche Zulässigkeit der Datenanwendung an sich hat, und sie nur eine individuelle Löschungspflicht des Widersprechenden bewirkt.

Im Fall der Weigerung des Auftraggebers, dem Widerspruch zu folgen, kann der Betroffene zB das Übermittlungsverbot als Folge eines rechtsgültigen Widerspruchs nur im Verfahren gemäß § 31 Abs 2 bei der DSK für den öffentlichen Bereich oder § 32 DSG 2000 bei den Landesgerichten für den privaten Bereich durchsetzen. Ein Verfahren für eine diesbezügliche Auseinandersetzung zwischen Auftraggeber und Betroffenen über die Berechtigung zum Widerspruch ist im konkreten Fall nicht vorgesehen.

Nach § 28 Abs 2 DSG 2000 kann der Betroffene gegen ein nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei (zB Telefonverzeichnis) jederzeit und ohne Begründung seines Begehrens Widerspruch erheben und die Daten sind sodann innerhalb von acht Wochen zu löschen. Was jedoch nicht bedeutet, dass zB ausgelieferte Telefonbücher wieder eingezogen, vernichtet und wieder neu gedruckt werden müssen. Dadurch soll nur gewährleistet werden, dass sinnvolle und nützliche Verzeichnisse dieser Art legal existieren können und dennoch auch abweichende Interessen von Betroffenen berücksichtigt werden können.

Im privaten Bereich, wo das Widerspruchsrecht den Charakter eines zivilrechtlichen Anspruchs aufweist, der auf dem Zivilrechtsweg durchgesetzt wird, ist auch ein (vorheriger, zB anlässlich der Datenermittlung vereinbarter) Verzicht auf die Ausübung des Widerspruchsrechts vorstellbar.⁴⁹⁸ Ein bereits in Kapitel .../Seite 70 (FN 103+104) angesprochenes mögliches Widerspruchsrecht von Bankkunden gegenüber ihrem Kreditinstitut entbehrt jedoch aufgrund der gesetzlichen Verpflichtung des Kreditinstituts nach § 39 BWG zur Risikovorsorge und im Interesse des Gläubigerschutzes einer an sich logischen Grundlage. (obwohl dies von der ARGE Daten verlangt wird)

Die Missachtung von diesbezüglichen Bescheiden der DSK oder Gerichtsurteile stellen sodann eine Verwaltungsübertretung iSd § 52 Abs 1 Z 3 DSG 2000 dar.

Gegen eine gesetzlich nicht angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit und ohne Nennung einer Begründung seines Rechtes, Widerspruch erheben. Das überwiegend schutzwürdige Geheimhaltungsinteresse wird gesetzlich vermutet. Öffentlich zugängliche Daten sind jene, in welche von jedermann unter den gleichen

⁴⁹⁸ *Duschanek*, Neuerungen und offene Fragen im DSG 2000, ZfV 2000/1303, 535

Bedingungen Einsicht genommen werden kann wie zB das Grund- und Firmenbuch. Allein das Bestehen einer Kostenpflicht für eine Abfrage sowie das Erfordernis, sich zum Nachweis der entrichteten Entgelte zu identifizieren, vermag die öffentliche Zugänglichkeit einer Datei nicht aufzuheben.⁴⁹⁹

14.3.1. Das Urteil OGH 6 Ob 195/08g

Ein auf dieser Rechtsansicht aufbauendes aktuelles Urteil⁵⁰⁰ stellt die Tätigkeit, Sinnhaftigkeit und Verlässlichkeit von Kreditauskunftsunternehmen in Frage. Sowohl das LGZ Wien als auch das Oberlandesgericht Wien als Berufungsgericht und nun auch der OGH hat bestätigt, dass jeder, über den kreditrelevante Daten gesammelt und entsprechende Auskünfte an andere erteilt werden, die Löschung dieser Daten verlangen kann. *"Betroffene Verbraucherinnen und Verbraucher haben einen Anspruch auf Löschung bonitätsrelevanter Daten aus einer öffentlich zugänglichen Datei. Dieses Widerspruchsrecht kann jederzeit ausgeübt werden und bedarf keiner Begründung"*, sagte der (ehemalige) Konsumentenschutzminister Erwin Buchinger, der den Verein für Konsumenteninformation mit dem Verfahren beauftragt hatte. Im Anlassfall wollte ein Konsument einen Vertrag mit einem Mobilfunkbetreiber abschließen. Der erkundigte sich bei einem Wirtschaftsauskunftsdienst über die Bonität des möglichen Kunden. Die Anfrage ergab drei negative Auskünfte - unter anderem über ein früheres Exekutionsverfahren gegen den Mann, mit dem offene Schulden hereingebracht werden sollten.

Der Vertrag wurde abgelehnt. Ebenso die Löschung der Negativ-/Exekutionsdaten durch die Auskunft, die der Mann daraufhin verlangte. Er machte damit von seinem Widerspruchsrecht nach § 28 iVm § 8 Abs 3 DSG 2000 Gebrauch. Weil er damit nicht durchdrang, klagte er den Auskunftsdienst auf Löschung der Daten und bekam Recht.

Werden Daten über die Kreditwürdigkeit in eine elektronische Datei aufgenommen, so hat der Betroffene ein Widerspruchsrecht im Sinne der Löschung dieser Daten. Die einzigen beiden Voraussetzungen für dieses Löschungsrecht sind erstens das Fehlen einer gesetzlich Anordnung, die Daten zu sammeln, und zweitens eine Aufnahme in eine öffentlich zugängliche Datei.

Der Berufung aufgrund unrichtiger rechtlicher Beurteilung wurde nicht stattgegeben.

Sowohl das OLG Wien als auch der OGH sah jedoch nicht die Ausführungen der Berufungsschrift für zutreffend an sondern bestätigte die rechtliche Beurteilung des

⁴⁹⁹ GZ K211.593/0011-DSK/2005 vom 29. November 2005

⁵⁰⁰ OGH 1.10.2008, 6 Ob 195/08g

Erstgerichts und die beiden materiellen Voraussetzungen des Widerspruchsrechts nach § 28 Abs 2 DSG 2000 als gegeben an:

1. Es existiert keine gesetzliche Anordnung zur Führung einer Datei über Bonitätsdaten iSd § 152 GewO. Das § 152 GewO dem § 28 Abs 2 GewO (formell oder) materiell derogiert, ist wegen des unterschiedlichen Regelungsinhaltes der genannten gesetzlichen Bestimmungen auszuschließen.
2. Es handelt sich um eine öffentlich zugängliche Datei, weil jeder Unternehmer mit berechtigtem Interesse auf Wunsch und gegen Entgelt (was unerheblich ist) Zugang zur Datenbank hat und nicht nur einem von vornherein bestimmten, nach außen hin begrenzten Personenkreis zugänglich ist. Als weitere Beispiele werden auch Verhandlungen vor einem Zivil- oder Strafgericht genannt welche „normalerweise“ öffentlich zugänglich sind jedoch zB für bewaffnete Zuhörer oder manchmal Unmündige nicht offen sind.

Das Widerspruchsrecht kann jederzeit auch ohne Begründung ausgeübt werden. Eine Interessensabwägung in Bezug auf schutzwürdige Interessen des Auftraggebers bzw. des Betroffenen ist nicht notwendig. Auch eine Begründung bei Nachfrage durch den Auftraggeber widerspricht dem Wortlaut des § 28 DSG 2000 und auch den Erläuterungen zur RV und den darin manifestierten Absichten des Gesetzgebers.⁵⁰¹

Der Gesetzgeber und eine große Mehrheit der Bevölkerung versteht die Existenz und Führung von Kreditinformationen/-evidenzen weil sie als sinnvoll und nützlich angesehen werden, andererseits sei es Ziel des Datenschutzgesetzes und iWS des Widerspruchsrechts, dem Betroffenen einen leicht durchsetzbaren Rechtsbehelf bei vom Durchschnitt abweichende Interessenslagen in die Hand zu geben.

Im Vergleich zu § 26 DSG 2000 erfordert § 28 DSG 2000 keinen Identitätsnachweis weil eine missbräuchliche Verwendung zum Nachteil Betroffenen mit sehr großer Wahrscheinlichkeit auszuschließen ist. Selbst die einmalige und konkrete Zustimmung des Betroffenen zur Einholung einer Bonitätsauskunft beschränkt dieses Widerspruchsrecht für die Zukunft nicht.

⁵⁰¹ ErläutRV GP XX 1613

Der Kläger kann durch die Ausübung seines Widerspruchsrechts sowohl seinen gesamten Datensatz als auch nur die ihn betreffenden negativen Auskünfte löschen. Ein nur auf Löschung der Negativeinträge ausgeübtes Widerspruchsrecht und damit eventuell verbundene Schadenersatzansprüche (welche bei der Auslegung des § 28 Abs 2 DSG keine Rolle spielen) von auskunftssuchenden Kunden der kreditgebenden Wirtschaft kann der Beklagte dadurch ausschalten, dass er von sich aus den gesamten Datensatz des Betroffenen löscht. Obwohl auch das OLG dem Beklagten zugesteht, dass durch das (fast) vorbehaltlose Widerspruchsrecht die von ihm geführte Datei an Aussagekraft verliert, ändert dies nichts an der Auslegung und klaren Aussagekraft des § 28 Abs 2 DSG 2000.⁵⁰²

Alle Auskunftsteile und Kreditschutzverbände hofften bis zum Schluss auf eine Korrektur des Urteils des OLG durch den OGH um dadurch einer Unzuverlässigkeit und Einschränkung der Aussagefähigkeit von Kreditinformationssystemen vorzubeugen. Dies wurde jedoch schließlich und endlich nicht erfüllt. Somit kann jeder Bürger der durch über ihn aufscheinende (in den meisten Fällen selbst verursacht) Negativinformationen an Vertragsabschlüssen gehindert wird, diese aus der jeweiligen Datenbank innerhalb von acht Wochen löschen lassen und danach als „unbescholtenes Blatt“ erneut dem gleichen Vertragspartner gegenüberstellen.

⁵⁰² www.diepresse.com, 17.7.2008

15. Sonderbestimmungen

15.1. Automatisierte Einzelentscheidungen

In Zeiten ständiger Rationalisierung und Automatisierung und der Verarbeitung von großen Datenmengen werden die Arbeitsabläufe in diesem Sinne auch angepasst. Jedoch verhindert § 49 DSG, dass Entscheidungen welche rechtliche Folgen für einen Betroffenen auslösen oder ihn in anderer Weise schwerwiegend beeinträchtigen, nicht rein maschinell getroffen werden dürfen und noch immer der menschlichen Einschätzung unterliegen. Diese gesetzliche Regelung zielt vor allem auf automatische Systeme ab welche etwa die berufliche Leistungsfähigkeit oder die Kreditwürdigkeit automatisiert beurteilen sollen. Daher dürfen z.B. Personalangelegenheiten oder die Vergabe von Krediten nicht ohne menschliche Mitwirkung entschieden werden. Nur aufgrund von Gesetzen, Verträgen oder anderen Sicherheiten, welche die Wahrung der Interessen des Betroffenen gewähren, dürfen diese ausnahmsweise auch ausschließlich automationsunterstützt getroffen werden.

Die Kommission führt in Bezug darauf wie folgt aus und hat dabei „Scoring“ Verfahren besonders im Blickfeld:

„So kann beispielsweise für die Kreditvergabe an eine Einzelperson auf die Technik des „credit scoring“ zurückgegriffen werden, wenn die positive Kreditvergabeentscheidung lediglich auf der Grundlage einer automatischen Risikobewertung ergehen; bei negativer Punktzahl muß die Wahrung der berechtigten Interessen der betroffenen Person garantiert werden (beispielsweise, wenn die endgültige Entscheidung ausgesetzt wird, bis die Dienste eine nicht automatische Prüfung der Akte vorgenommen haben können).“⁵⁰³

Verstöße gegen § 49 DSG 2000 befinden sich zwar nicht im Widerspruch zum Grundrecht auf Datenschutz weil die Zulässigkeit der betreffenden Verarbeitung gegeben sein wird, jedoch werden Daten entgegen den Bestimmungen des DSG verwendet. Der Betroffene hat somit gegenüber dem Auftraggeber des privaten Bereichs Anspruch auf Unterlassung und Beseitigung vor dem Zivilgericht geltend zu machen. Verletzungen des § 49 DSG 2000 unterliegen keiner Verwaltungsstrafsanktion.⁵⁰⁴

Die rechtliche Ausgestaltung von Art 15 DS-RL bleibt dem nationalen Gesetzgeber überlassen. Ein unmittelbares Verbot solcher Entscheidungen ist allerdings nicht zwingend

⁵⁰³ Vgl. Begründung der Kommission zur Art 15 des geänderten Vorschlages der Kommission, ABl. EG Nr. C 311 vom 27.11.1992, 27

⁵⁰⁴ Duschaneck, DSG 2000, 150ff

weil Art 15 Abs 1 DS-RL davon spricht, dass die Mitgliedsstaaten jeder Person das Recht einräumen sollen, nicht durch eine automatisierte Einzelentscheidung beeinträchtigt zu werden.⁵⁰⁵ Es soll daher diesen Personen ein subjektives Recht eingeräumt werden, was gegen die Entscheidung spricht solche Entscheidungen prinzipiell zu verbieten. Die Richtlinie fordert weiters eine „erhebliche Beschwer“ welche durch eine automatisierte Einzelentscheidung verursacht wird. Dies wird idR durch den Erhalt von Prospekten nicht gegeben sein aber sehr wohl bei Fälligestellung eines Kredits, Nichtberücksichtigung bei einer freien Stelle, Versagung einer behördlichen Genehmigung, etc.⁵⁰⁶

Sollte eine betroffene Person Auskunft darüber verlangen, so ist der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen.⁵⁰⁷ *Dammann* ist der Ansicht, dass aufgrund der überwiegenden Verwendung von komplexer und damit komplizierter Standardsoftware in den meisten Unternehmen der Hinweis auf das benutzte Programm oder System nicht weiterhilft.⁵⁰⁸

15.2. Data-mining, Data-warehousing

In den letzten Jahren kommt es bei Mobilfunkbetreibern, Banken und Versicherungsgesellschaften, Supermarktketten und Versandhäusern auch zum vermehrten Einsatz von „Data-Mining“ welches jedoch nicht nur als Marketinginstrument sondern auch als automatisierte Beurteilung der Kundenbonität verwendet wird. Darunter versteht man die Erfahrungen und Charakteristika aus der Vergangenheit zu nutzen um zu errechnen welche Kunden statistisch gesehen zu Rückzahlungsausfällen oder Zahlungsverzögerungen tendieren. Wenn man mit anonymisierten Daten arbeitet und nur gruppenspezifische, statistische Aussagen macht, entsteht diesbezüglich jedoch kein Problem in Bezug auf den Datenschutz.⁵⁰⁹ Andererseits wird hier jedoch auch mit persönlichen Daten hantiert deren Verwendung der Kunde zuvor nicht für einen bestimmten Zweck autorisiert hat. Werden jedoch wahllos Daten in großen Datenbanken gesammelt (Data warehousing) , diese zu einem späteren (noch unbestimmten) Zeitpunkt analysiert (Data mining) ist dies aufgrund des

⁵⁰⁵ So *Dammann/Simitis*, Art 15, Rn 1; aA *Brühmann/Zerdick*, CR 1996, 429 (433) die darin überhaupt ein Verbot von automatisierten Einzelentscheidungen erblicken

⁵⁰⁶ *Ehmann/Helfrich*, EG DS-RL, Art 15 Rn 7, 18+19; ebenso *Dammann/Simitis*, EG DS-RL, Art 15 Rn 7

⁵⁰⁷ *Souhrada-Kirchmayer*, Datenschutzgesetz, 945

⁵⁰⁸ *Burgsdorff*, Die Umsetzung der EG DS-RL im nicht öffentlichen Bereich, 65; *Dammann/Simitis*, EG DS-RL, Art 12 Rn 8 geben jedoch keine Auskunft darüber, welche Informationen dem Betroffenen in concreto überhaupt helfen würden, den Verarbeitungsprozess zu verstehen. Sinnvoll wären Angaben über die einzelnen Schritte, in denen die Daten für deinen Vorgang benutzt werden und der Betroffene zu mindestens in der Lage ist, die genauen Ziele und Zwecke der Datenverarbeitung zu erkennen.

⁵⁰⁹ Der Standard, 28.6.2004

Zweckbindungsgrundsatzes nicht zulässig. Auch die Vorratsdatenbeschaffung widerspricht dem Zweckmäßigkeitssatz, weil der Zweck der Datenermittlung ja vorher festgelegt werden muss. (§ 6 Abs 1 Z 2 DSG 2000)⁵¹⁰

⁵¹⁰ *Baeriswyl*, Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut ?, RdV 2000, 6; *Weichert*, Datenschutzrechtliche Anforderungen an Data-Warehouse-Anwendungen bei Finanzdienstleistern

15.3. Informationsverbundsystem

Um besseren Kundenservice bieten zu können und auch die Zugriffsmöglichkeiten zu erhöhen, haben Unternehmen in manchen Branchen ein Informationssystem aufgebaut bei dem der Betreiber des Informationssystem die Daten einspeichert und sie jedem Systemteilnehmer (heute fast überall mittels internet) zur Verfügung stellt. Dies betrifft die schon oben genannten Informationssysteme der Kreditauskunfteien (siehe Kapitel 10. + 11.) aber auch interne Unternehmensnetzwerke.

Der Gesetzgeber hat diesen Informationssystemen aufgrund der Gefährdung für den einzelnen Betroffenen eine eigene Definition zuteil werden lassen welche in § 4 Z 13 DSG 2000 zu finden ist:

Ein Informationsverbundsystem ist

- 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 werden.

Ein Informationsverbundsystem liegt demnach nicht vor, wenn ein Auftraggeber – Dienstleister - Verhältnis besteht oder wenn die Daten von einem Auftraggeber an den anderen übermittelt werden.

Liegt hingegen keine der beiden oben genannten Tatbestände vor und befinden sich die Daten in einem Unternehmensnetzwerk, auf das jeder auf sämtliche Daten Zugriff hat, so liegt mit ziemlicher Sicherheit ein Informationsverbundsystem vor. Entscheidend ist hier vor allem das Vorhandensein von Zugriffsberechtigungen welche eine strikte Abgrenzung der Daten von einzelnen Unternehmen(-steilen) ermöglichen und dadurch den Begriff des Informationsverbundsystems negieren.⁵¹¹

Liegt dagegen ein Informationsverbundsystem vor, so sind eine Reihe von Auflagen zu erfüllen:

- Vor Inbetriebnahme ist eine Vorabgenehmigung durch die DSK nach § 18 Abs Z 4 einzuholen, andernfalls drohen Verwaltungsstrafen bis zu € 9.445,-- (§ 52 Abs 2 DSG 2000)

⁵¹¹ Knyrim, Datenschutzrecht, 22 ff

- Der Auftraggeber eines Informationsverbundsystems hat nach § 50 Abs 1 DSG 2000 einen geeigneten Betreiber zu bestellen und an das DVR zwecks Eintragung zu melden. Dieser Betreiber kann einer der beteiligten Auftraggeber sein oder ein Dritter. Jeder daran beteiligte Auftraggeber hat seine Teilnahme gesondert bei der DSK zu melden.
- Der bestellte Betreiber hat die Pflicht, innerhalb von zwölf Wochen jedem Betroffenen auf Antrag alle Auskünfte zu geben, die notwendig sind um sein Rechtsschutzbedürfnis zu befriedigen.
- Der Betreiber haftet für die notwendigen Maßnahmen zur Datensicherheit iSd § 14 DSG 2000 (mit der Ausnahmeregelung des § 33 Abs 3 DSG 2000)
- Wird ein Informationsverbundsystem betrieben, ohne dass eine Meldung an die DSK unter Angabe eines Betreibers erfolgt ist, so treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers (§ 50 Abs 1 DSG 2000)
- Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten auf den Betreiber übertragen werden. Sofern dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber den Betroffenen und den für die Vollziehung dieses BG zuständigen Behörden nur wirksam, wenn er – aufgrund einer entsprechenden Meldung an die DSK – aus der Registrierung im DVR ersichtlich ist (§ 50 Abs 2 DSG 2000)

16. Rechtsschutz

Kommt der Rechtsträger seinen Pflichten auf Auskunftserteilung nicht nach, kann im Rahmen des privaten automationsunterstützten Datenverkehrs auf Auskunft die Datenschutzkommission (DSK) eingeschaltet werden.⁵¹² (§§ 1 Abs. 3 Z 1 und 26 iVm 31 DSG 2000) Mit Klage kann auf Unterlassung der rechtswidrigen Verarbeitung, Benützung oder Übermittlung von Daten sowie die Beseitigung des dadurch hergestellten rechtswidrigen Zustandes begehrt werden, unabhängig von eventuellen (zivilrechtlichen) Schadenersatzansprüchen. Die Klage auf Unterlassung setzt weder objektive Sorgfaltswidrigkeit noch Verschulden voraus; das Vorliegen von Wiederholungsgefahr, das idR vermutet wird, ist ausreichend (vgl § 32 Abs 2 DSG 2000, § 13 UWG). Diese wird typischerweise durch eine „Einstweilige Verfügung“ iSv §§ 378, 381 EO veranlasst werden.⁵¹³ Im Anwendungsbereich des DSG 2000 wird der Zugang zur „Einstweiligen Verfügung“ noch insoweit erleichtert, als deren Erlassung vom Vorliegen der Voraussetzungen des § 381 EO unabhängig ist, also insbesondere auch ohne den Nachweis eines drohenden unwiederbringlichen Schadens beantragt werden kann (vgl dazu § 32 Abs 3 DSG 2000).

Bei Gefahr in Verzug wegen „wesentlicher Gefährdung schutzwürdiger Geheimhaltungsinteressen“ kann die DSK die Weiterführung mit Mandatsbescheid gem § 57 Abs 1 AVG untersagen (§ 20 Abs 2 DSG 2000); dagegen ist nur eine Vorstellung an die DSK selbst zulässig (§ 40 Abs 1 DSG 2000 iVm § 57 Abs AVG)

Der Betroffene hat jedoch gegenüber dem Auftraggeber Anspruch auf

- Rechtmäßigkeit der Ermittlung (§ 6 Abs 1 Z 2 DSG 2000)
- Rechtmäßigkeit der Verarbeitung (§ 7 Abs 1 DSG 2000)
- Rechtmäßigkeit der Übermittlung (§ 7 Abs 2 DSG 2000)
- Datengeheimnis (§ 15 ➔ § 52 Abs 1 Z 2 DSG 2000)
- Datensicherung (§ 14 ➔ § 52 Abs 2 Z 4 DSG 2000)
- Auskunft (§ 26 ➔ § 52 Abs 1 Z 3 DSG 2000)

⁵¹² Die Zuständigkeit der DSK – und nicht der ordentlichen Gerichte – für Auskunftsbeschwerden im privaten Bereich war ein erklärtes Ziel des DSG 2000: „Um auch bei der Aufrechterhaltung des geteilten Rechtsschutzsystems eine Vereinfachung des Zugangs zum Rechtsschutz für die Betroffenen zu bewirken, soll jedoch das Recht auf Auskunft – unabhängig davon, ob der belangte Auftraggeber dem öffentlichen oder dem privaten Bereich zuzurechnen ist – in Hinkunft vor der DSK durchsetzbar sein. Dies scheint deshalb so wichtig, weil der Inhalt der Auskunft in den meisten Fällen entscheidend ist für die Frage, ob der Betroffene Sinnvollerweise ein Verfahren wegen Löschung, Berichtigung oder Unterlassung der Verwendung anstrengen soll“ (1613 BeilNR XX GP)

⁵¹³ Canaris, Bankvertragsrecht I³, Rz 70

- Rückersatz des Entgelts (§ 26 Abs 6 DSG 2000)
- Richtigstellung und Löschung (§ 27 → § 52 Abs 1 Z 3 SG 2000)

Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen und beim jeweiligen Landesgericht einzubringen, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Wohnsitz hat. Er hat jedoch auch die Wahl am Sitz oder Aufenthaltsort (des Auftraggebers oder Dienstleister des Landesgerichtes für Zivilrechtssachen zu klagen. (§ 32 Abs 4 DSG 2000) Es besteht Anwaltszwang. Es besteht daher für den Betroffenen im Falle des Unterliegens bei Gericht das volle Prozess- und Kostenrisiko.

Im Grundrechtstatbestand des § 1 DSG 2000 wird nicht ausdrücklich zwischen den beiden Bereichen unterschieden; bei den besonderen Voraussetzungen für behördliche Grundrechtseingriffe und der Zuweisung von Aufgaben des Rechtsschutzes an die ordentlichen Gerichte oder an die DSK ist nicht die rechtliche Organisationsform des Auftraggebers, sondern die Datenverwendung „*in Vollziehung der Gesetze*“, also ein funktionieller Gesichtspunkt maßgeblich. (§ 1 Abs 5 DSG 2000) ⁵¹⁴

Die Vornahme einer Löschung, Richtigstellung, Widerruf oder die Erteilung einer Auskunft sind Handlungen die der Natur nach nicht durch einen Dritten vorgenommen werden können sondern alleine durch den Verpflichteten. (unvertretbare Handlung, ohne Ersatzvornahmemöglichkeit). Eine Vollstreckung derartiger unvertretbaren Handlungen ist in den §§ 354 und 355 EO geregelt.

Sämtlichen genannten Ansprüchen, Beschwerden oder Klagen ist gemeinsam, dass der Anspruch innerhalb eines Jahres nach Kenntnis vom beschwerenden Ereignis, erlischt. Längsten falls aber binnen drei Jahren, nachdem das behauptete Ereignis stattgefunden hat. Eine diesbezügliche Beschwerde, Eingabe oder Klage wird nach Fristablauf von der DSK bzw. vom Gericht abgewiesen (§ 34 Abs 1 DSG 2000)

Bei Ansprüchen gegenüber Auftraggeber des öffentlichen Bereichs soweit sie nicht ein Organ der Gesetzgebung oder der Gerichtsbarkeit betreffen, wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts hat die Datenschutzkommission (DSK) in einem Verfahren in Bescheidform zu entscheiden. (§ 1 Abs 5 DSG 2000)

⁵¹⁴ Duschaneck § 1 DSG in Korinek/Holoubek, Österr BfVR – GR III, Rz 36, 52ff, 86ff

Sollte sich der öffentliche Auftraggeber auf geschützte Interesse iSd §§ 26 Abs 5 oder 27 Abs 5 berufen, so hat nach Überprüfung der Notwendigkeit der Geheimhaltung der geschützten öffentlichen Interessen die Behörde durch Bescheid zu entscheiden. Gegen die Entscheidung der DSK kann die belangte Behörde Beschwerde an den VfGH erheben.

Wenn die Verletzung eines Grundrechts behauptet wird, kann nach Erschöpfung des Instanzenzuges (wenn die Entscheidung in Bescheidform ergangen ist), direkt an den VfGH nach Art 144 B-VG oder in Form einer unmittelbaren Gesetzes- oder Verordnungsanfechtung nach Art 140 bzw 139 B-VG, herangetreten werden.⁵¹⁵

Weiters wird neben der gerichtlichen und der Zuständigkeit der Datenschutzkommission auch die Möglichkeit der Klage eines Betroffenen bei einer Aufsichtsbehörde der Wirtschaft für Datenverarbeitungen welche mit der Ausübung einer Konzession o.ä. im Zusammenhang stehen, in Betracht kommen und diese dann bescheidmäßig untersagen kann. (zB Untersagung eines Vereines wegen Überschreitung des satzungsmäßigen Vereinsgegenstandes).⁵¹⁶

Bisher eher unbekannt ist die Tatsache, dass die DSK bei Beschwerden in jüngster Zeit bei Unternehmen vor Ort durch das „Zentrum für sichere Informationstechnologie-Austria“ (A-SIT, reg. Verein, BPD Wien ZVR 948166612) als Amtssachverständigen Augenscheine durchführen und Gutachten erstellen hat lassen.⁵¹⁷

Durch § 30 DSG 2000 wurde ein Kontrollverfahren (auch als „Ombudsmann Verfahren“ bezeichnet) eingeführt betreffend den privaten und öffentlichen Bereich eingeführt, das zwar nur von der betroffenen Person angestoßen werden kann, aber nicht auf die (behauptete) Verletzung subjektiver Rechte beschränkt ist. So können im privaten Bereich Verletzungen des Rechts auf Geheimhaltung, Richtigstellung oder Löschung, auf deren Einhaltung der Betroffene kein subjektives (dh einklagbares) Recht hat, mithilfe dieses Ombudsmann Verfahrens wirksam bekämpft werden. Bei vorabkontrollpflichtigen Datenanwendungen kann ein solches auch ohne Vorliegen einer Eingabe oder auch nur eines konkreten Verdachts durchgeführt werden.

Im öffentlichen Bereich kann der Betroffene wählen, ob er ein rechtsförmliches Verfahren oder ein Ombudsmann Verfahren anstrebt. Bestimmte Auftraggeberpflichten, welchen kein

⁵¹⁵ Siehe hiezu die stRsp VwSlgNF 7194 A, 7096 A/1967 und VfSlg 4816/1964, VfSlg 12.880/1991; mit dem Vorwurf der Gesetzlosigkeit, denkumögliche Gesetzesanwendung oder Anwendung eines verfassungswidrigen Gesetzes (sog. „Grundrechtsformel“)

⁵¹⁶ H. Schäfer, Wirtschaftsaufsicht ÖZW 1978, 7ff; ÖZW 1979/1,18

⁵¹⁷ zB GZ K120.813/0006-DSK/2005 vom 7. Juni 2005; GZ K120.839/005-DSK/2005 vom 21. Juni 2005; GZ K120.908/0009-DSK/2005 vom 26. November 2004

subjektives Recht auf Seiten des Betroffenen gegenübersteht (zB Meldepflicht an das DVR), können nur im Rahmen eines Verfahrens nach § 30 DSG 2000 wirksam eingemahnt werden.⁵¹⁸

Ziel ist nach § 30 Abs 6 DSG 2000 die Herbeiführung eines rechtmäßigen Zustands. Dazu können nötigenfalls auch – nicht unmittelbar verbindliche – Empfehlungen ausgesprochen werden. Häufig kann aber auch ohne den Einsatz dieses Mittels im Zuge solcher Verfahren eine datenschutzrechtlich befriedigende Situation hergestellt werden wenn sich die Eingabe nicht schon von vornherein als unbegründet erweist.⁵¹⁹ Eine Empfehlung der DSK zur Herstellung des rechtmäßigen Zustandes iSd § 30 Abs 6 DSG 2000 hat jedoch keinen normativen Charakter und ist daher kein Bescheid.⁵²⁰

Aus Abs 2 ergibt sich auch die Zuständigkeit der DSK bei begründetem Verdacht, Prüfverfahren (samt Einschau) bei Datenverarbeitungen durchzuführen. Prinzipiell muss aber auch festgehalten werden, dass bei Nichtvorliegen einer Standard- oder Musteranwendung der Auftraggeber nach § 17 Abs 1 DSG 2000 verpflichtet ist, VOR Aufnahme einer Datenanwendung eine Meldung an die DSK zum Zwecke der Registrierung im DVR zu erstatten. Bei Datenverarbeitungen die der sog. „Vorabkontrolle“ iSd § 18 Abs. 2 DSG 2000 unterliegen⁵²¹, das sind jene Verarbeitungstypen mit besonderen datenschutzrechtlichen Gefährdungspotential⁵²² wie auch zB Daten über die Kreditwürdigkeit der Betroffenen (§ 18 Abs 2 Zi 3 DSG 2000) , kann auch von Amts wegen, ohne Vorliegen einer Eingabe eines Betroffenen eine Zuständigkeit begründet werden. Dabei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung die notwendige Aufklärung verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren (§ 30 Abs 3 DSG 2000).

Die Formblätter für diese Meldung sind vom DVR bzw. unter der Internetadresse <http://www.dsk.gv.at/site/6296/default.aspx> abrufbar. Eine Meldung ist auch auf

⁵¹⁸ DSB 2005, 16

⁵¹⁹ DSB 2007, 40ff

⁵²⁰ VwGH 19.12.2006, Zl. 2006/06/0301 (gegen die Erledigung der Datenschutzkommission vom 29. September 2006, GZ K213.000/0005-DSK/2006)

⁵²¹ Zum Anwendungsbereich der Vorabkontrolle ausführlich ErläutRV zu § 18

⁵²² Erwägungsgrund 53 der RL nennt darin, dass eine Verarbeitung dazu dient, Betroffene von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrages auszuschließen (Hauptfälle: credit scoring im Kreditwesen, Warndateien in der Versicherungsbranche); so auch *Gounalakis/Mand*, CR 1997, 497 (500)

elektronischem Weg per @mail möglich (dvr@dsk.gv.at) und kostenlos. Wenn innerhalb von zwei Monaten kein Auftrag zur Verbesserung erteilt wird, gilt die Meldepflicht als erfüllt. (§ 18 Abs 2 iVm § 20 Abs 3 und 5 DSG 2000)

Zur Vermeidung von Verzögerungen hat die DSK die Prüfung innerhalb von zwei Monaten vorzunehmen; wird innerhalb dieser Frist seitens der DSK dem Auftraggeber kein Verbesserungsauftrag erteilt, muss die Registrierung durchgeführt werden und kann die Verarbeitung aufgenommen werden. (§ 20 Abs 1 und 5 DSG 2000) Die DSK hat mit Bescheid auch Auflagen zu erteilen, soweit dies zur Wahrung durch das DSG 2000 geschützten Interessen der Betroffenen notwendig ist. (§ 21 Abs 2 DSG 2000)

Wird den Empfehlungen nicht entsprochen, kann die DSK auch jede weitere geeignete Maßnahme zur Herstellung des gesetzmäßigen Zustands ergreifen wie zB amtswegige (Wieder-)Eröffnung eines Registrierungsverfahrens, Erstattung von Anzeigen an die zuständige Strafbehörde und im privaten Bereich bei begründeten Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber, anstelle des Betroffenen auch eine Feststellungsklage iSd § 228 ZPO beim zuständigen Zivilgericht erheben.⁵²³ (§ 32 Abs 5 DSG 2000)

Nach § 32 Abs 6 hat die DSK überdies, wenn ein Betroffener es verlangt und es zu Wahrung der nach diesem BG geschützten Interessen einer größeren Zahl von Betroffenen geboten ist, einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient iSd §§ 17ff ZPO⁵²⁴ beizutreten. Der Beitritt dient zur Wahrung von geschützten Interessen welche sich aus den §§ 1, 26, 27 und 28 DSG 2000 ergeben können. Der DSK obliegt zwar keine meritorische Entscheidung über diese Ansprüche, jedoch müssen im Antrag Indizien für das aufrechte Bestehen diese Ansprüche vorliegen. Hierbei handelt es sich um eine einfache Nebenintervention, dh die DSK ist nur Streithelfer ohne Parteistellung, die Urteilswirkungen erstrecken sich nur auf den Betroffenen. Im Urteil kann auch ausgesprochen werden, dass es im DVR einzutragen ist, wenn es für eine größere Anzahl von Betroffenen von Bedeutung ist. Damit wird zwar keine Wirkung des Urteils auf andere Betroffene als den Kläger erzielt, doch ein öffentlicher Hinweis auf die Rechtmäßigkeit oder Rechtswidrigkeit von Verarbeitungen gegeben.⁵²⁵

⁵²³ DSB 2001, 10; *Duschanek/Rosenmayr-Klemen*, Datenschutz – Regierungsvorlage, *ecolex* 1999, 364

⁵²⁴ § 17 ZPO lautet: (1) Wer ein rechtliches Interesse daran hat, dass in einem zwischen anderen Personen anhängigen Rechtsstreite die eine Person obsiege, kann dieser Partei im Rechtsstreite beitreten (Nebenintervention).

(2) Zu solchem Beitritte sind ferner alle Personen befugt, welchen durch gesetzliche Vorschriften die Berechtigung zur Nebenintervention eingeräumt ist.

⁵²⁵ *Pawlikowsky*, Datenschutz, Leitfaden & Materialien, 71

Aus dem § 32 DSG 2000 kann ein zwingender Charakter der Bestimmungen nicht angenommen werden. Im Rahmen der zivilrechtlichen Vorschriften ist daher eine Einschränkung der Haftung auch im Zusammenhang mit dem DSG 2000 möglich. Im Rahmen des § 104 JN⁵²⁶ kann auch eine im Rahmen des § 32 DSG 2000 liegende Gerichtsvereinbarung zwischen Betroffenen und Auftraggeber getroffen werden. Aus § 104 Abs JN geht jedoch zweifelsfrei hervor, dass Rechtssachen, die den Gerichtshöfen erster Instanz zugewiesen sind, durch Vereinbarung nicht vor ein Bezirksgericht gebracht werden können. Aber weder § 104 JN noch § 32 DSG 2000 verhindern, dass durch Vereinbarung der gewünschte Gerichtshof erster Instanz vereinbart werden kann.⁵²⁷

526 § 104 JN lautet: 1) Die Parteien können sich durch ausdrückliche Vereinbarung unterwerfen:

1. der inländischen Gerichtsbarkeit;
2. einem oder mehreren Gerichten erster Instanz namentlich angeführter Orte.
Die Vereinbarung muß urkundlich nachgewiesen werden; eine sonstige Voraussetzung muß nicht erfüllt sein.
- (2) Die Vereinbarung hat nur dann rechtliche Wirkung, wenn sie sich auf einen bestimmten Rechtsstreit oder auf die aus einem bestimmten Rechtsverhältnisse entspringenden Rechtsstreitigkeiten bezieht. Jedoch können Angelegenheiten, welche dem Wirkungskreise der ordentlichen Gerichte überhaupt entzogen sind, durch solche Vereinbarungen nicht vor diese Gerichte, Rechtssachen, welche vor ein Bezirksgericht gehören, nicht vor einem Gerichtshof erster Instanz und ausschließlich den Gerichtshöfen erster Instanz zugewiesene Streitigkeiten nicht vor ein Bezirksgericht gebracht werden.
- (3) Ein an sich auf Grund des Fehlens der inländischen Gerichtsbarkeit oder der sachlichen oder örtlichen Zuständigkeit unzuständiges Gericht wird auch dadurch zuständig, dass der Beklagte zur Sache vorbringt (§ 74 ZPO) oder mündlich verhandelt, ohne die Einrede des Fehlens der inländischen Gerichtsbarkeit oder der sachlichen oder örtlichen Zuständigkeit zu erheben, sofern er dabei durch einen Rechtsanwalt oder einen Notar vertreten ist oder sofern er vorher durch den Richter über die Möglichkeit einer derartigen Einrede und deren Wirkung belehrt und diese Belehrung im Verhandlungsprotokoll beurkundet worden ist.
- (4) In Rechtssachen nach den §§ 81, 83, 83b und 92b kann die inländische Gerichtsbarkeit nach den Abs. 1 oder 3 nicht begründet werden.
- (5) Die Abs. 1 bis 4 sind insoweit zur Gänze oder zum Teil nicht anzuwenden, als nach Völkerrecht oder besonderen gesetzlichen Anordnungen ausdrücklich anderes bestimmt ist.

527 Hanreich, in Datenschutz in der Wirtschaft, Zivilrechtliche Probleme des DSG, 81ff

17. Strafbestimmungen

- a) Verwaltungsstrafrechtliche Bestimmungen
- b) Zivilrechtliche Bestimmungen (siehe oben u.a. Schadenersatz)
- c) Strafrechtliche Bestimmungen

17.1. Verwaltungsstrafrechtliche Bestimmungen

Die verwaltungsstrafrechtliche Haftung wird aufgrund § 9 Abs 1 Verwaltungsstrafgesetz (VStG) geregelt. Demnach sind für juristische Personen verwaltungsstrafrechtlich verantwortlich jene die zur Vertretung nach außen berufen sind. Das sind bei einer GesmbH gemäß § 18 GmbHG die Geschäftsführung, bei einer AG nach § 71 AktG der Vorstand.

Nach § 9 Abs 2 und Abs 3 VStG kann die Verantwortlichkeit nach bestimmten räumlichen oder sachlichen Kriterien auf bestimmt verantwortliche Personen übertragen werden. Um eine tatsächliche verwaltungsstrafrechtliche Haftbarkeit zu gewährleisten, muss der verantwortliche Beauftragte gemäß § 9 Abs 4 VStG folgende Voraussetzungen erfüllen:

- seinen Wohnsitz im Inland bzw. EWR Staat haben
- strafrechtlich verfolgt werden können
- der Bestellung nachweislich zugestimmt haben
- eine klare Abgrenzung des Verantwortungsbereichs ausdrücklich vorgenommen und zugewiesen wurde.

Fehlt jedoch nur eine dieser Voraussetzungen, so kann der Beauftragte verwaltungsrechtlich nicht zur Verantwortung gezogen werden und es bleibt die Verantwortung der zur Vertretung nach außen befugten Personen (idR Geschäftsführer/Vorstand) bestehen.

Verletzt der verantwortliche Beauftragte auf Grund einer besonderen Weisung des Auftraggebers eine Verwaltungsvorschrift, so ist er dann nicht verantwortlich, wenn er glaubhaft zu machen vermag, dass ihm die Einhaltung dieser Verwaltungsvorschrift unzumutbar war (§ 9 VStG Abs 5)

Die zur Vertretung nach außen berufenen Personen iSd Abs 1 sowie Personen im Sinne des Abs 3 bleiben trotz Bestellung eines verantwortlichen Beauftragten – auch im Falle der

Anstiftung und Beihilfe iSd § 7 - strafrechtlich verantwortlich, wenn sie die Tat vorsätzlich nicht verhindert haben. (§ 9 VStG Abs 6)

Juristische Personen und eingetragene Personengesellschaften sowie die in Abs 3 genannten natürlichen Personen haften für die über die zur Vertretung nach außen Berufenen oder über einen verantwortlichen Beauftragten verhängten Geldstrafen, sonstige in Geld bemessene Unrechtsfolgen und die Verfahrenskosten zur ungeteilten Hand. (§ 9 VStG Abs 7)

Zuständig für die Vollziehung der Verwaltungsstraftatbestände ist die Bezirksverwaltungsbehörde in deren Sprengel der Auftraggeber seinen gewöhnlichen Hauptsitz oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission (DSK) eingerichtete Bezirkverwaltungsbehörde zuständig. Zweite Instanz ist der UVS.

17.2. Zivilrechtliche Bestimmungen

17.2.1. Schadenersatz

In Umsetzung von Art 23 Abs 1 DS-RL haftet der Auftraggeber gegenüber dem Betroffenen nach den Bestimmungen des bürgerlichen Rechts, wenn er ihm schuldhaft und rechtswidrig durch Verwendung von Daten Schaden zufügt (§ 33 DSG 2000). In der Literatur ist die Auslegung von Art 23 DS-RL allerdings umstritten.⁵²⁸ Es sollte darin eine Erfolgshaftung mit Befreiungsgründen normiert werden. In den meisten Fällen kommt in Österreich jedoch das Prinzip der Verschuldenshaftung iSd §§ 1293ff ABGB zur Geltung.⁵²⁹ Es wird weiters unterschieden zwischen

a) *realer Schaden* – tatsächliche Veränderung im Vermögens- und Persönlichkeitsbereich des Geschädigten welche im Sinne einer Wiederherstellung (Naturalrestitution) wieder ausgeglichen werden soll

b) *positiver Schaden* – Schädigung an bestehenden Vermögensgütern und Rechten

⁵²⁸ aA Dammann/Simitis, EG DS-RL, 264 welche darin eine verschuldensunabhängige Haftung erblicken; bejahend dagegen Ehmann/Helfrich, EG DS-RL, 280 f; Duschaneck/Rosenmayr-Klemenz, DSG RV, ecolex 1999, 364 sprechen auch von einer Beweislastumkehr (aA Mayer-Schönberger, 224)

⁵²⁹ Mayer-Schönberger, Information und Recht: vom Datenschutz bis zum Urheberrecht, 221ff und die hL sieht in Art 23 DS-RL eine verschuldensunabhängige Haftung die jedoch vom österreichischen Gesetzgeber falsch umgesetzt und in eine verschuldensabhängige Haftung mit einer zusätzlichen Exulpierungsmöglichkeit normiert wurde

- c) *entgangener Gewinn* – zukünftige Erwerbs- und Gewinnchancen werden zu Nichte gemacht; Ersatz nur bei Vorsatz oder grober Fahrlässigkeit
- d) *ideeller oder immaterieller Schaden* – nicht in Geld messbarer Schaden wie Reputation, Ansehen, Trauer,..... Ersatz in Geld nur in gesetzlich geregelten Ausnahmefällen

Das DSG 2000 verweist auf die allgemeinen Bestimmungen des bürgerlichen Rechts. Nach dem ABGB wird ein Schaden nur ersetzt, wenn folgende Voraussetzungen gegeben sind:⁵³⁰

- Eintritt eines Schadens. Nach dem ABGB wird ursprünglich nur ein tatsächlicher Vermögensschaden ersetzt, nicht jedoch ein ideeller Schaden (abgesehen von Schmerzensgeld bei Körperverletzungen). Seit dem ZivRÄG 2004 (173 BlgNR XXII.GP.) wird durch § 1328a⁵³¹ normiert, dass bei jeder schuldhaften und rechtswidrigen Verletzung der Privatsphäre der Ersatz auch immaterieller Schäden zusteht.⁵³² § 33 DSG 2000 ist als „lex specialis“ zu sehen und sollte daher der allgemeinen, als Auffangtatbestand gesehenen Norm des § 1328a vorangehen. (Abs 2 leg cit)
- Der Verstoß gegen das DSG 2000 muss kausal für den Schadenseintritt sein.
- Der Verstoß muss weiters schuldhaft dh persönlich vorwerfbar sein
- Wer bei vorsätzlicher oder grob fahrlässiger rechtswidriger Verhaltensweise einen anderen schädigt, hat das *Interesse* (=entstandener positiver Schaden unter Beachtung der konkreten, subjektiven Umstände plus entgangener Gewinn [1324 ABGB]) zu ersetzen
- Bei leicht fahrlässiger Schädigung ist nur der positive Schaden (am objektiv berechneten gemeinen Wert der Sache zum Zeitpunkt der Schädigung) zu ersetzen (§1323 ABGB)

⁵³⁰ Ausführlich hiezu *Kozio/Welser*, Bürgerliches Recht II, 13. Aufl.

531 § 1328a lautet: (1) Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, hat ihm den dadurch entstandenen Schaden zu ersetzen. Bei erheblichen Verletzungen der Privatsphäre, etwa wenn Umstände daraus in einer Weise verwertet werden, die geeignet ist, den Menschen in der Öffentlichkeit bloßzustellen, umfasst der Ersatzanspruch auch eine Entschädigung für die erlittene persönliche Beeinträchtigung.

(2) Abs. 1 ist nicht anzuwenden, sofern eine Verletzung der Privatsphäre nach besonderen Bestimmungen zu beurteilen ist. Die Verantwortung für Verletzungen der Privatsphäre durch Medien richtet sich allein nach den Bestimmungen des Mediengesetzes, BGBl. Nr. 314/1981, in der jeweils geltenden Fassung.

⁵³² Vgl. OGH 16 Os 6,7/91 der auch die Gehaltshöhe hier mit einbezieht weil daraus Rückschlüsse auf die privaten Verhältnisse möglich sind; ausführlich *Helmich*, Schadenersatz bei Eingriffen in die Privatsphäre, *ecolex* 2003, 888ff; *Lukas*, Schadenersatz bei Verletzung der Privatsphäre, *RZ* 2004, 33ff

Für Geschäfts- und Betriebsgeheimnisse besteht in Österreich kein absolutes Recht und auch keine mit § 1328a ABGB vergleichbare Norm.⁵³³ In Deutschland wurde hingegen ein Recht am Gewerbebetrieb anerkannt, dass als bloßes Rahmenrecht aber noch die Rechtswidrigkeit zu begründen aufgibt (Interessensabwägung).⁵³⁴ Der OGH hält jedoch den Schutz des wirtschaftlichen Rufes auch gegenüber wertender Unternehmenskritik für möglich, was aber die bloße Tatsachenmitteilung nicht erfasst.⁵³⁵ Ein Schutz des Unternehmens gegen wahre Behauptungen wird jedenfalls abzulehen sein, wenn die Mitteilung einem berechtigten Informationsinteresse dient.⁵³⁶ Für Fälle schwerwiegender oder rechtswidriger Datenverwendung, die ihrem Wesen nach Tatbeständen vergleichbar sind, die nach dem Mediengesetz zum Schadenersatz verpflichtet, ist bei Verwendung von sensiblen Daten, strafrechtlich relevanten Daten oder Auskunft über die Kreditwürdigkeit der Ersatz immateriellen Schadens vorgesehen. Die näheren Voraussetzungen und die Höhe der Entschädigung ergeben sich aus den §§ 6 und 7 MedienG⁵³⁷ und können bis zu € 20.000 betragen. Die Höhe der Entschädigung ist gemäß § 6 Abs 1 Satz 2 MedienG nach Maßgabe des Umfangs und der Auswirkungen der Veröffentlichung, insbesondere auch der Art und des Ausmaßes der Verbreitung des Medium zu bestimmen.

Ein ideeller Schadenersatz ist daher nur unter den folgenden drei Voraussetzungen zulässig und möglich:

1. eine öffentlich zugängliche Verwendung
2. von sensiblen und in § 18 Abs 2 DSG 2000 weiters angeführten besonders schutzwürdigen Daten
3. eine Verletzung der Geheimhaltungsinteressen des Betroffenen, die der Bloßstellung nach § 7 Abs 1 MedienG gleichkommt.

Diese Regelung geht über die Vorgaben der Datenschutz RL hinaus.⁵³⁸ Wie im ABGB haften auch nach dem DSG 2000 der Auftraggeber und der Dienstleister für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war. (§ 33 Abs 2 DSG 2000)

⁵³³ Honsell in Ruppe (Hrsg), Geheimnisschutz im Wirtschaftsleben (1980), 45ff

⁵³⁴ Rebhahn, Geheimnisschutz-Datenschutz-Informationsschutz, 17; Palandt/Sprau, § 823 BGB (2007) Rz 126 ff

⁵³⁵ zB OGH SZ 61/93

⁵³⁶ Haybäck, Können wahre Tatsachenbehauptungen Ehrenbeleidigungen iSd § 1330 ABGB sein?, JBl 1994, 732

⁵³⁷ BGBl 1981/314 idF BGBl I 2007/112

⁵³⁸ Dammann/Simitis, EG DS-RL, 263 bejahend; differenziert Ehmann/Helfrich, EG DS-RL, 282f mwH, die den nationalen Gesetzgeber dazu verpflichtet sehen diesbezüglich Stellung zu beziehen

Entsprechend der Datenschutz RL besteht eine Beweislastumkehr; der Auftraggeber hat demnach nachzuweisen, dass der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten nicht zur Last gelegt werden kann. Der Einwand, dass die Datenschutz RL eine verschuldensunabhängige Haftung verlangt und § 33 DSG 2000 demnach gegen Gemeinschaftsrecht verstößt⁵³⁹ kann mit Hinweis auf Art 23 Abs 2 Datenschutz RL beantwortet und entkräftet werden. Eine Haftungsbefreiung durch den Nachweis, dass dem Auftraggeber der schadensverursachende Umstand „nicht zur Last gelegt“ werden kann, erscheint nur im Falle einer Verschuldenshaftung sinnvoll.⁵⁴⁰

Dammann–Simitis führen aus, dass aufgrund der Datenschutz RL immaterieller Schadenersatz in unbegrenzter Höhe von den Mitgliedsstaaten zu gewähren ist. Dies wird damit begründet, dass die Mitgliedsstaaten gemäß Art 23 der Datenschutz RL Regelungen einzuführen haben, nach denen jede Person, der aufgrund einer rechtswidrigen Datenverarbeitung Schaden entsteht, das Recht hat, Schadenersatz zu verlangen. Die Richtlinie spricht von „Schadenersatz“, ohne dazu irgendwelche weiteren Präzisierungen vorzunehmen. Die Schadenersatzpflicht dürfe deshalb einerseits nicht begrenzt werden und andererseits wären sowohl materielle als auch immaterielle Schäden ersatzpflichtig.⁵⁴¹

Der Anspruch auf Behandlung einer Beschwerde verjährt nach Ablauf eines Jahres ab Kenntnis des Betroffenen, längstens aber binnen dreier Jahre, nachdem das Ereignis behauptetermaßen stattgefunden hat. (§ 34 Abs 1 DSG 2000)

17.2.2. Das Urteil LGZ Wien 53 Cg 106/07h vom 15.2.2008

In Fortführung des in Kapitel 1./Seite 12 genannten Sachverhaltes, kam es in weiterer Folge zu einem Gerichtsverfahren wo Herr Dr. Anton K. seine Forderung auf immateriellen Schadenersatz nach dem DSG 2000 an den Verein für Konsumenteninformation (VKI) abtrat. Im Urteil **LGZ Wien, 15.02.2008 53 Cg 106/07h** wurde sodann Herrn Dr. Anton K. ein immaterieller Schadenersatz in der Höhe von € 750,-- zugesprochen.

Unter Hinweis auf § 33 Abs 1 DSG 2000 urteilte das Gericht, dass der betroffene Auskunftsdienst dem Konsumenten wegen schuldhafter Verwendung seiner Daten entgegen

⁵³⁹ *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000, 38

⁵⁴⁰ *Duschanek*, Neuerungen und offene Fragen im DSG 2000, ZfV 2000/1303, 536 sowie *Ehmann/Helfrich*, EG DS-RL, Kurzkomentar (1999), 280 mwH; aM *Brühann*, Kommentierung der DS-RL, in: *Grabitz/Hilf/Wolf* (Hrsg), Kommentar zur Europäischen Union, RZ 5 zu Art 23 (ohne Begründung)

⁵⁴¹ *Dammann-Simitis*, EG-Datenschutz Richtlinie, 263; *Kilches*, DSG 2000-Selbstbestimmter Datenschutz Neuerungen aufgrund der Datenschutz RL 95/46/EG, MR 1999, 261

den Bestimmungen des DSG den erlittenen (immateriellen) Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen hat. Werden durch die öffentlich zugängliche Verwendung der in den § 18 Abs 2 Zi 1 bis 3 DSG 2000 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung⁵⁴² gemäß § 7 Abs 1 Mediengesetz gleichkommt, so gilt diese Bestimmung auch in den Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Gemäß § 33 Abs 2 haftet der Auftraggeber und der Dienstleister auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

Im § 6 Abs 1 Z 1 DSG 2000 ist der Grundsatz verankert, dass Daten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden dürfen. Dieser Grundsatz erfordert eine entsprechende Benachrichtigung des Betroffenen, um ihm die Möglichkeit zu geben, sich gegen eine seiner Meinung nach nicht gerechtfertigte, seine Kreditwürdigkeit massiv beeinträchtigende Datenverwendung zur Wehr zu setzen. Eine derartige Verständigung ist in diesem Falle (so wie eigentlich in fast allen Fällen) nicht erfolgt. (siehe auch Kapitel 10.5.1.). Die Aufnahme der hier in Rede stehenden Eintragung in die Datenbank der Beklagten ist somit rechtswidrig erfolgt und sie ist der Firma auch subjektiv vorwerfbar, weil Herr Dr. Anton K. bereits vor dieser Eintragung in die Datenbank Kontakt mit dem Inkassounternehmen, welche in Vertragsbeziehung zur Beklagten steht, aufgenommen und die Forderung dem Grunde nach bestritten hat. Schon zu diesem Zeitpunkt hätte klar sein müssen, dass die Nichtbezahlung auf keinen Fall ein geeignetes Zeichen darstellt über die Kreditwürdigkeit des Betroffenen urteilen zu können. Dem Einwand des Beklagten, die Datei sei nicht öffentlich, weil sie nur einem begrenzten Personenkreis zugänglich gemacht wird, wurde vom Gericht nicht gefolgt, weil die Datenbank einem nicht von vornherein bestimmten, nach außen hin nicht begrenzten Personenkreis zugänglich gemacht wird und der Zugang nur von der Entscheidung des Auftraggebers über das ausreichende „berechtigte Interesse“ des Abfragenden abhängig ist.

Die Forderung stammte weder aus einer vertraglichen Beziehung noch wurde sie von Herrn Dr. Anton K. akzeptiert und daher auch bestritten. Nachdem diese Negativmeldung geeignet war, das berufliche Fortkommen des Betroffenen zu gefährden oder zu beeinträchtigen, jedoch diese Daten nur in geringem Umfang verwendet wurden, wurde die Schadenersatzleistung von € 750,-- als angemessen angesehen.

⁵⁴² Bloßstellen bedeutet, Tatsachen aus seinem höchstpersönlichen Lebensbereich (wozu auch die Daten nach § 18 Abs 2 Z 1 bis 3 DSG 2000 gehören) zu enthüllen, die ihn aus der Sicht Dritter herabsetzen und sein Ansehen untergraben. Siehe *Dohr-Pollirer-Weiss*, Datenschutzrecht², § 33 Rz 3 f

17.2.3. Weitere zivilrechtliche Bestimmungen

Weiters ist auch noch auf die Bestimmung des § 1330 Abs 2 ABGB hinzuweisen, die eine Haftung für die Verbreitung unwahrer Tatsachen vor, die den Kredit, den Erwerb oder das Fortkommen gefährden. Bedingung ist jedoch, dass der Verbreiter die Unwahrheit kannte oder kennen musste.⁵⁴³ Die Aufzählung darin ist auch nicht abschließend sondern nur exemplarisch. Unter „Kredit“ wird generell die finanzielle Bonität, unter „Erwerb“ jede gewinnorientierte wirtschaftliche Tätigkeit, verstanden.⁵⁴⁴ Der Begriff des „beruflichen Fortkommens“ orientiert sich am strafrechtlichen Inhalt und umfasst die Möglichkeit, eine verantwortungsvollere und damit in der Regel besser entlohnte Position anzustreben und zu erreichen.⁵⁴⁵ Der Anwendungsbereich umfasst jedoch nicht nur ehrenrührige sondern auch rufschädigende Äußerungen. Andererseits ist der Schutzzumfang soweit eingeschränkt, dass nur unwahre Tatsachenbehauptungen nicht aber Werturteile umfasst und darunter subsumiert werden können. Weiters ist die Haftung für nicht bewusst unwahre, vertrauliche Informationen ausgeschlossen, wenn der Äußernde oder der Empfänger daran ein berechtigtes Interesse haben. Dabei ist an die Beurteilung der Vertraulichkeit ein strenger Maßstab anzulegen. Ein berechtigtes Interesse besteht, wenn die Information für die persönlichen, gesellschaftlichen oder wirtschaftlichen Beziehungen oder Verhältnisse von Bedeutung ist oder an der Mitteilung der Information ein öffentliches Interesse besteht.⁵⁴⁶ Der Gesetzgeber erkennt zwar den wirtschaftlichen Ruf als Persönlichkeitsrecht an, stuft jedoch seinen Schutz ab und gewährleistet diesen nur unter bestimmten Umständen. Dies führt bei den Auskunftfeien zu einer Vertypung eines „Standard-Sachverhalts“ und zu einer weiteren Abstufung der zivilrechtlichen Haftung.⁵⁴⁷

Im Verhältnis zwischen Ehrenbeleidigung und Rufschädigung besteht nach jüngerer hL und mittlerweile stRsp Anspruchskonkurrenz. Wird der wirtschaftliche Ruf iSd § 1330 Abs 2 ABGB verletzt so besteht neben Anspruch auf Unterlassung, der von Rechtswidrigkeit und Verschulden des Eingriffs unabhängig ist, auch Anspruch auf Ersatz des (materiellen)

⁵⁴³ OGH 13.10.1995, MR 1996, 26ff

⁵⁴⁴ *Reischauer in Rummel*, Rz 7 zu § 1330 ABGB; *Korn/Neumayer*, Persönlichkeitsschutz im Zivil- und Wettbewerbsrecht, 35ff

⁵⁴⁵ *Hager/Walenta*, Persönlichkeitsschutz, 23; OGH 25.9.1984, ÖBl 1985, 6 – Betrugsvorwurf; OGH 26.1.1988, MR 1988, 87

⁵⁴⁶ OGH 20.10.1987, MR 1988, 84 – Alpenländischer Kreditorenverband; OGH 9.7.1987, MR 1987, 171 – Pille danach; OGH 29.9.1988, MR 1989, 12 – Alpenländischer Kreditorenverband II; OGH 31.8.1983, ÖBl 1984, 18 = EvBl 1984/60 – Lokomotivführer; *Zeiler*, Persönlichkeitsschutz, 17ff

⁵⁴⁷ *Mayer-Schönberger*, Information und Recht: Vom Datenschutz bis zum Urheberrecht, 32; *G.Korn*, Die zivilrechtliche Ehrenbeleidigung, MR 1991, 138 sieht darin eine „Schutzvorschrift zugunsten des Geschäftsverkehrs“;

entstanden Schadens. Ein immaterieller Schadenersatz ist diesbezüglich ausgeschlossen. Mit dem Schutz der Ehre hat der Schutz des wirtschaftlichen Rufes gemein, dass dem Betroffenen „durch falsche Informationen Gefahren drohen“.⁵⁴⁸

Wer, indem er ohne Befugnis in fremde Rechte eingreift, die von der Rechtsordnung einem anderen zugewiesen wurden, einen Vorteil gezogen hat, muss diesen dem so Verkürzten zurückgeben. Das ist der Kern des Verwendungsanspruchs nach § 1041 ABGB.⁵⁴⁹

Hiermit soll der Inhaber eines subjektiven Rechts geschützt werden, dass ein ihm zugewiesener Vorteil einem anderen zufließt. Ich möchte hier auf die bereicherungsrechtlichen Ansprüche in Bezug auf das geschützte Werk, Bild- und Namensrechte sowie am Brief nicht weiter eingehen und auf die Anwendung des § 1041 ABGB auf das subjektive Recht auf Datenschutz kurz thematisieren.

Die Existenz einer vermögensrechtlichen Dimension beim subjektiven Recht auf Schutz der eigenen personenbezogenen Daten ist abhängig von der Zuweisung eines Ausschließungsgrundes an den Betroffenen durch die Rechtsordnung sowie von der Verknüpfung der personenbezogenen Informationen mit einem konkreten wirtschaftlichen Wert am Markt. Aufgrund des DSG 2000, welches der vierten Generation zuzurechnen ist, kann jedenfalls von einem den übrigen Rechten an Information vergleichbaren Ausschließungsrecht gesprochen werden. Bei Auskunftgebern und Adressverlagen werden personenbezogene Daten in detail wie zB Einkommen, Bildungsgrad, Darlehenshöhe, Automarke, etc. Dritten gegen Entgelt zur Verfügung gestellt und stellen damit einen wirtschaftlichen Wert am Markt dar. Es steht daher bei unbefugten Eingriffen ein Verwendungsanspruch iSd § 1041 ABGB zu. Der Anspruchsumfang richtet sich nach der Redlichkeit des Bereicherten.⁵⁵⁰ Der Verwendungsanspruch richtet sich somit nicht nur gegen den der rechtswidrig gehandelt hat, sondern auch gegen einen Dritten, der sie in der Folge rechtmäßig gutgläubig erhalten.

17.3. Strafrechtliche Bestimmungen

⁵⁴⁸ OGH 9.1.1990, MR 1990, 57 – Arbeitsunfall; *Zeiler*, Persönlichkeitsschutz, 1 und 21; OGH 13.4.1983, SZ 56/83; OGH 10.4.1991, ÖBl 1991, 161 – Altöl Skandal; *Frick*; Persönlichkeitsrechte, 103; OGH 31.8.1983, ÖBl 1984, 18 = EvBl 1984/60 – Lokomotivführer

⁵⁴⁹ *Koziol-Welser*, Grundriss, 13. Aufl., 415ff; § 1041 spricht zwar von „Eigentümer“ doch ist dieser Begriff (genau so wie der Begriff „Sache“) weit auszulegen und meint damit jeden, „dem ein Rechtsgut zugeordnet ist“

⁵⁵⁰ *Mayer-Schönberger*, Information und Recht: vom Datenschutz bis zum Urheberrecht, 191 (198ff); zu ausführlichen Erklärung des Verwendungsanspruchs siehe *Koziol-Welser*, Grundriss I, 13. Auflage, 415ff

Zum Schutz von Daten und Computersystemen enthält das StGB mehrere Bestimmungen, die hohe Geld- und sogar Freiheitsstrafen bis zu 10 Jahre vorsehen:

- § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem
- § 119a StGB Missbräuchliches Abfangen von Daten
- § 126a StGB Datenbeschädigung
- § 126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten
- § 148a StGB Betrügerischer Datenverarbeitungsmissbrauch
(§ 51 DSG 2000 ist diesem sehr ähnlich)

Zu beachten ist, dass sowohl § 126a als auch § 148a StGB in die Liste der in § 166 StGB „Begehung im Familienkreis“ privilegierten Delikte aufgenommen wurde und dadurch die Privatanklage und ein erheblich geringeres Strafausmaß wirksam werden. Ebenso kann bei diesen Delikten der Strafaufhebungsgrund der Täterin Reue iSv § 167 StGB zum Tragen kommen.

Im Gegensatz zu §§ 118a und § 119a StGB, die gem § 74 Abs 2 StGB sowohl personenbezogene als auch nicht personenbezogene Daten umfassen, ist § 51 DSG auf den Schutz personenbezogener Daten beschränkt. Hinzuweisen ist noch auf die Tatsache, dass § 3 StGB die notwehrfähigen Güter taxativ aufzählt und daher gelten Privatsphäre (und Briefgeheimnis) als nicht notwehrfähig. Die Lehre zählt jedoch auch Geschäftsgeheimnisse zum notwehrfähigem Vermögen.⁵⁵¹

Weitere Bestimmungen welche im weiteren Sinn Daten schützen (sollen):

- § 119 StGB Verletzung des Telekommunikationsgeheimnisses
- § 121 StGB Verletzung von Berufsgeheimnissen
- § 122 StGB Verletzung eines Geschäfts- oder Betriebsgeheimnisses
- § 123 StGB Auskundschaftung eines Geschäfts- und Betriebsgeheimnisses
- § 124 StGB Auskundschaftung eines Geschäfts- und Betriebsgeheimnisses zugunsten des Ausland
- § 310 StGB Verletzung des Amtsgeheimnisses⁵⁵²
- § 101 BWG Verletzung des Bankgeheimnis

⁵⁵¹ Kienapfel, Strafrecht AT (2007), Z 11 Rz 6; Lewisch, WK-StGB² (2004), § 3 Rz 41; zum Vermögen einschränkend Reischauer in Rummel, ABGB³ (2004), § 19 Rz 6

⁵⁵² Vgl hierzu auch Schmölzer, Strafrecht, in: Jähnel/Schramm/Standegger, Informatikrecht (2000), 255 u. 263 mwH; Wagner, Unbefugter Zugriff auf e-mail, ecolex 2000, 273

18. Exkurs - Das Bankgeheimnis

Nachdem durch Bonitätsauskünfte auch das Bankgeheimnis zu mindestens indirekt tangiert wird, möchte ich auf den nächsten folgenden Seiten die grundlegendsten Dinge in Bezug auf das Bankgeheimnis und die Bankauskunft hervorheben.

Bereits im Jahr 1765 in Art 19 des „Reglements der Königlichen Giro- und Lehn Banco“ Friedrichs des Großen heißt es:

*„Wir verbieten bey Unserer Königlichen Ungnade allen und jeden nachzuforschen, wie viel ein anderer auf sein Folium zu Gute habe, auch soll niemand von denen Bancoschreibern sich unterstehen, solches zu offenbaren, weder durch Worte, Zeichen oder Schrift, bey Verlust ihrer Bedienungen und bei denen Strafen, die meyneidige zu erwarten haben. Zu dem Ende soll sie bey Antretung ihres Amtes besonders schwören, dass sie alle die Geschäfte, die sie als Bediente der Banco unter Händen haben werden, als das größte Geheimnis mit in die Grube nehmen werden.“*⁵⁵³

Bis 1979 war die Bankverschwiegenheit lediglich auf vertraglicher Grundlage anerkannt und es bestanden mangels positivrechtlicher Klärung erhebliche Zweifel, ob und wie weit das Bankgeheimnis auch gegen gesetzliche Offenbarungs- und Auskunftspflichten geltend gemacht werden konnte oder musste.⁵⁵⁴ Erst mit dem KWG 1979⁵⁵⁵ ist eine Klarstellung des Umfanges des Bankgeheimnisses, eine wesentliche Erweiterung des Kreises der Verpflichteten und eine besondere Strafbestimmung eingeführt worden. Weiters hat man das Konzept der Bankverschwiegenheit auf eine neue Grundlage gestellt indem man die bloße Verschwiegenheitspflicht zu einer allgemeinen Auskunftsverweigerungspflicht gemacht hat, die sich mangels besonderer Ausnahmenvorschriften grundsätzlich und generell gegen alle sonstigen gesetzlichen Offenbarungs- bzw. Auskunftspflichten richtet und daher auch gegenüber behördlichen Auskunftsverlangen wirksam ist.⁵⁵⁶ Zuvor gab es nur zwei spezielle

⁵⁵³ Zitiert nach Claussen, Bank- und Börsenrecht³ (2003), § 6 Rz 2

⁵⁵⁴ Schinnerer-Avancini, Bankverträge³, I, 176ff; Jabornegg-Strasser-Floretta, Das Bankgeheimnis, 24ff

⁵⁵⁵ BGBl 1979/63, in Kraft getreten am 1.3.1979

⁵⁵⁶ Zur neuen Konzeption Jabornegg-Strasser-Floretta, Das Bankgeheimnis, 26ff

Vorschriften und zwar in § 22 Abs 3 des Postspargesetzes sowie im Depotgesetz aus 1969 welche somit als Vorbild fungiert haben dürften.⁵⁵⁷

*„Hätte das römische Recht bereits das Bankgeheimnis gekannt, hätte es nicht so ausführliche Bestimmungen über den Schatzfund treffen müssen. Dank dem (neuen) KWG ist eine Einlage bei einer österreichischen Kreditunternehmung ebenso geheimnisgeschützt wie ein vergrabener Schatz.“*⁵⁵⁸

Bald nach Inkrafttreten des KWG kam es zu Hausdurchsuchungen und zur Beschlagnahme von Unterlagen bei Banken, die im Zuge von Finanzstrafverfahren durchgeführt wurden aber auch Unbeteiligte betrafen. Ein Erlass des BMF hielt diese Vorgangsweise jedoch für gesetzmäßig und betonte insbesondere, dass die zusätzlich gefunden Unterlagen weiteren Strafverfahren zugrunde gelegt werden dürfen.⁵⁵⁹ Werner Doralt meinte in Bezug auf die Rechtsauffassung des BMF „dass ein einziger Steuerpflichtiger gegen den ein Strafverfahren lauf, ausreiche, um das zweitbeste Bankgeheimnis der Welt aus den Angeln zu heben“⁵⁶⁰. Der VfGH hat in seinem Erkenntnis vom 7.12.1983 diese Ansicht bestätigt worauf *Werner Doralt* dies als „Ende des Bankgeheimnisses im Abgabenverfahren überhaupt“ kommentierte.⁵⁶¹

Doch schon ein Jahr später entschied der VfGH⁵⁶² im Zuge einer Überprüfung der Beschlagnahmenvorschriften des § 89 Abs 1 und Abs 2 FinStrG, dass diese verfassungskonform insoweit auszulegen sind, dass eine Beschlagnahme von Beweismittel nicht zulässig sei wenn dadurch eine berufliche Verschwiegenheitspflicht umgangen wird. Obwohl dieses Erkenntnis nicht zum Bankgeheimnis ergangen war, wurde daraus abgeleitet, dass die Rechtsansicht des VfGH dadurch überholt sei und durch eine verfassungskonforme Interpretation das Bankgeheimnis wieder hergestellt sei.⁵⁶³ Dieses VfGH Erkenntnis war jedoch Anlass für den Gesetzgeber die Beschlagnahmenvorschriften des FinStrG zu novellieren und sich erneut mit der Absicherung des Bankgeheimnisses zu beschäftigen.⁵⁶⁴

⁵⁵⁷ *Jabornegg-Strasser-Floretta*, Das Bankgeheimnis, 18ff

⁵⁵⁸ So *W. Ulrich*, in *Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben, 283

⁵⁵⁹ Erlass des BMF vom 3.12.1979 FS-130/1-III/9/79, abgedruckt bei *W. Doralt*, Das Bankgeheimnis im Abgabenverfahren (1982), 55ff

⁵⁶⁰ *W. Doralt*, Das Bankgeheimnis im Abgabeverfahren, ÖJZ 1981, 652 in Anlehnung an eine Äußerung Bruno Kreiskys, wonach das Bankgeheimnis in Österreich „das zweitbeste der Welt, gleich nach den Bermudas“ sei.

⁵⁶¹ VfGH 7.12.1983, 82/13/0082; ÖStZB 1984, 309; RdW 1984, 128

⁵⁶² VfGH 3.12.1984, G24/83; G50/83; G51/83; G52/83; G89/83; G107/84

⁵⁶³ *Arnold*, Aktuelles zum Bankgeheimnis, ÖBA 1985, 19ff; *Beiser*, Beschlagnahme von Klientenunterlagen verfassungswidrig, ÖStZ 1985, 24

⁵⁶⁴ BGBl 571; *Jabornegg*, Neues zum Bankgeheimnis, WBl 1990, 29

Auch noch heute besteht für die FMA kein unüberprüfbares freies Ermessen bankgeheimnisrelevante Daten ohne unmittelbaren persönlichen und sachlichen Zusammenhang zu erfragen.⁵⁶⁵ Es scheint sich daher die Ansicht durchzusetzen den Umfang des Bankgeheimnisses in Anlehnung an den Datenschutz⁵⁶⁶, im Sinne einer Interessensabwägung zu begrenzen.

Im Jahr 1988 wurde das Bankgeheimnis als Verfassungsbestimmung abgesichert. (damals als § 35a KWG; nunmehr § 38 Abs 5 BWG) Eine Änderung bzw gar Abschaffung kann nur mit erhöhten Quoten von ½ Präsenz- und 2/3 Konsensquorum vorgenommen werden.⁵⁶⁷ Das BWG ist ein Wirtschaftsaufsichtsgesetz. Ebenso wie das zuvor gültige KWG 1979 beruht dieses auf dem Kompetenzbestand des Art 10 Z 5 B-VG.⁵⁶⁸ Es kommt dabei idR nicht auf das wirtschaftsrechtliche Gepräge einer Norm an ob die Regelung in privat- oder öffentlich-rechtlicher Form erfolgt.⁵⁶⁹ Lt hL können wirtschaftsrechtliche Angelegenheiten in beiden Formen kodifiziert werden wodurch es aufgrund der Unschärfe des BWG bezüglich des Bankgeheimnisses in Bezug auf dessen Rechtsnatur zu diversen literarischen Kontroversen kam.⁵⁷⁰ Aufgrund der Verpflichtung der Kreditinstitute auch ohne ausdrückliche gesetzliche Normierung, in Folge eines Geschäftsbesorgungsverhältnis,⁵⁷¹ Stillschweigen zu bewahren, ist eine privatrechtliche Deutung nahe liegend. Andererseits führt die Einbettung in das BWG zu einer Überlagerung durch das Aufsichtsrecht durch die FMA welche Verstöße dagegen zu ahnden hat.⁵⁷²

Seit 1. Jänner 1994 gilt betreffend das Bankgeheimnis die Regelung des § 38 Bankwesengesetz – BWG, BGBl 1993/532. Das Bankgeheimnis für sich alleine vermittelt kein subjektives Recht. Ein Anspruch entsteht erst im Umweg über das Grundrecht auf Datenschutz iSd § 1 DSG 2000.⁵⁷³ Als schutzwürdige Interessen iSv § 1 Abs 1 DSG 2000

⁵⁶⁵ *Jabornegg*, Aktuelle Fragen des Bankgeheimnisses, ÖBA 1997, 668ff verweist im Zusammenhang mit § 41 Abs 2 BWG (Geldwäscherei) auf das verfassungsrechtliche Legalitätsprinzip und die Systematik der sonstigen Fälle der Durchbrechung des Bankgeheimnisses

⁵⁶⁶ In § 1 Abs 2 DSG 2000 ist die Interessensabwägung – im Gegensatz zu § 38 BWG – ausdrücklich erwähnt

⁵⁶⁷ Bereits die Vorgängerregelung des § 23 KWG orientierte sich an Art 14 Abs 10 B-VG; EB zur RV, ÖStZ 1988, 180

⁵⁶⁸ *Brünner-Pauper*, Das System des Rechts der österreichischen Kreditwirtschaft, 160ff; ebenso die EB zur RV zum KWG 1979, 844 BlgNR XIV. GP, 35f

⁵⁶⁹ *Schwark*, Anlegerschutz durch Wirtschaftsrecht (1979), 67 sieht die Differenzierung in der Gesetzgebungspraxis von nachrangiger Bedeutung; für ihn ist die Zweckmäßigkeit und die Höhe der zu entstehenden Kosten entscheidend

⁵⁷⁰ Der OGH sieht die Geheimhaltungspflicht zu § 23 Abs 1 KWG als privatrechtliche Vorgabe; siehe dazu auch *Apathy/Iro/Koziol*, BVR I (2007) Rz 2/2

⁵⁷¹ Vgl *Apathy*, in *Schwimmann* (Hrsg), ABGB Praxiskommentar³ (2006), § 1009 Rz 6

⁵⁷² Näher dazu *Schwark* in *Anlegerschutz durch Wirtschaftsrecht* (1979), 276ff

⁵⁷³ So *Oppitz*, in *Geheimnisschutz – Datenschutz – Informationsschutz*, ÖZW 2006, 125

bzw überwiegend berechtigter Interessen iSv § 1 Abs 2 DSG 2000 werden alle verfassungsgesetzlichen gewährleisteten Rechte anzusehen sein⁵⁷⁴. Ein berechtigtes Interesse muss auf jeden Fall auf eine Rechtsnorm rückführbar sein.⁵⁷⁵

Im engeren Sinn ist darunter die gesetzliche Verpflichtung jedes Mitarbeiters eines Kreditinstituts zu verstehen, über die finanziellen Verhältnisse von Kunden absolutes Stillschweigen zu bewahren wobei zu beachten ist, dass das Bankgeheimnis Geheimnisse aufgrund der Geschäftsverbindung mit Kunden schützt, während das DSG alle in einem Bankbetrieb vorhandenen personenbezogenen Daten in seinen Wirkungsbereich mit einbezieht. Obwohl Art 8 EMRK eine im Verfassungsrang stehende Grundlage für den Schutz zumindestens bestimmter bankgeheimnisrelevanter Daten im Gewand des Rechts auf Geheimhaltung der Privat- und Familiensphäre bietet, gibt es ein Grundrecht auf Wahrung des Bankgeheimnisses freilich nicht doch kann § 1 DSG 2000 im Rahmen seines Anwendungsbereiches durchaus als verfassungsgesetzliche Grundlage des Anspruchs auf Wahrung des Bankgeheimnisses qualifiziert werden.⁵⁷⁶ Obwohl die Verwendung des unbestimmten Begriffes des „*Privatlebens*“ zu Unschärfe führt und dadurch den Charakter einer „Generalklausel“ vorgibt, macht es dieser in weiterer Folge unmöglich eine Abgrenzung durchzuführen weil der Mensch in seiner jetzigen gesellschaftlichen Position in verschiedenartigen Beziehungen zur seiner Umwelt auftritt.⁵⁷⁷

Die Preisgabe von Informationen, die das Privat- und Familienleben betreffen, stellt noch keine Verwirkung des Schutzes nach Art 8 EMRK dar, soweit die Bank als Empfängerin dieser Informationen selbst einer Verschwiegenheitspflicht unterliegt. Da die Bank Trägerin des Geheimnisses ist, kann der Staat seinen Auskunftsanspruch gegen die Bank nur unter den selben Bedingungen geltend machen, unter denen er an den Kunden selbst herangetreten durfte.⁵⁷⁸ Daher darf ein Eingriff des Staates in das Bankgeheimnis grundsätzlich nur auf der Grundlage von Gesetzen erfolgen, die den Art 8 Abs 2 EMRK genannten Bedingungen entsprechen. Da die Rechte aus der EMRK auch durchsetzbar sind, musste der Gesetzgeber

⁵⁷⁴ Rill, Das Grundrecht auf Datenschutz in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, 15ff

⁵⁷⁵ Laurer, Der Geheimnisschutz im österreichischen Grundrechtssystem, EuGRZ 1983, 34 (FN 10), 36; Dohr-Pollirer-Weiss, DSG, Anm 13 zu § 1 DSG (1979); aA Rill, Das Grundrecht auf Datenschutz in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, 22, der auch gesellschaftliche Wertungen einbeziehen will

⁵⁷⁶ Weissel, Das Bankgeheimnis in der österreichischen Grundrechtsordnung, ÖZW 1989, 80ff der die Bestimmung des § 35a KWG als Unikat im Bereich des Geheimnisschutzes tituliert; mit Verweis auf Potyka, Datenschutz im Kreditwesen, in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft (1981), 121, 129ff

⁵⁷⁷ Stolzlechner, Der Schutz des Privat- und Familienlebens im Licht der Rechtsprechung des VfGH und der Straßburger Instanzen, ÖJZ 1980, 88; Ermacora, Grundriss der Menschenrechte in Österreich, Rz 353ff; Berka, Medienfreiheit und Persönlichkeitsschutz, 296

⁵⁷⁸ Berka, Medienfreiheit und Persönlichkeitsschutz, 302; Laurer, Der Geheimnisschutz im österreichischen Grundrechtssystem, EuGRZ, 34; Wenger, Grundriss des Wirtschaftsrecht, Rz 363

auch Vorkehrungen treffen, dass sich der Bankkunde gegen eine Verletzung seines Anspruchs auf Achtung seines Privatlebens angemessen zur Wehr setzen kann.⁵⁷⁹ Auskunftsansprüche von Privatpersonen durchbrechen das Bankgeheimnis bereits bei Vorliegen berechtigter Interessen, die dem schutzwürdigen Geheimhaltungsinteresse des Kunden vorgehen.⁵⁸⁰

Der OGH⁵⁸¹ definiert „Geheimnisse“ wie folgt:

„Tatsachen, Vorgänge oder Verhältnisse tatsächlicher oder rechtlicher Natur, die nur einem verhältnismäßig beschränkten Personenkreis bekannt und zu wahren sind, wenn es das Interesse dessen, auf den sich das Bankgeheimnis bezieht, erfordert.“

Weiters führt er in einem anderen Judikat dazu aus: *„Was ein Geheimnis ist, ist den allgemeinen Rechtsgrundsätzen zu entnehmen. Dazu gehört vor allem, dass die geheimhaltungsbedürftige Tatsache nur einem begrenzten Personenkreis bekannt ist und auch bekannt sein soll.“*⁵⁸²

Ähnlich, in Anlehnung an der von *Burgstaller* gegebenen „Standarddefinition“ des Geschäfts- und Betriebsgeheimnisses zum (damaligen) § 23 KWG:⁵⁸³

„Geheimnisse sind Tatsachen, die bloß einer bestimmten und begrenzten Zahl von Personen bekannt und anderen nicht oder nur schwer zugänglich sind, die nach dem Willen der betroffenen Person nicht über den Kreis der Eingeweihten hinaus dringen sollen und deren Offenbarung nicht zur Verfolgung berechtigter Interessen der Kreditunternehmung erforderlich ist.“

Ähnlich auch *Arnold*⁵⁸⁴ der *„Tatsachen aufgrund der Geschäftsverbindung anvertraut und zugänglich gemacht sieht, sobald sie in einem inneren Zusammenhang mit dem Bankgeschäft stehen und der Bank infolge eines Tätigwerdens den Kunden oder eines Dritten bekannt geworden sind. Umstände, die die Bank auf andere Art und Weise in Erfahrung gebracht hat, unterliegen nicht der Geheimhaltungspflicht nach § 23 KWG“*

⁵⁷⁹ VfGH 3.12.1984, G 24, 50-52, 89/83, 107/84 = VfSlg 10.291/1984 = EuGRZ 1985, 94ff mit Anm *Kopetzki* = AnwBl 1985, 43ff, mit auch auf die Auswirkungen auf den Geheimnisschutz hinweisender Anm von *Arnold*

⁵⁸⁰ *Weissel*, Das Bankgeheimnis in der österreichischen Grundrechtsordnung, ÖZW 1989/3, 87

⁵⁸¹ OGH 8.3.1988, 3 Ob 559/86, EvBl 1989/1 – ergangen zu § 23 KWG

⁵⁸² OGH 2.2.1984, 6 Ob 613/83, SZ 57/29; OGH 8.3.1988, 3 Ob 559/86, EvBl 1989/1; OGH 25.2.1992, 4 Ob 114/91, EvBl 1992/58; vgl. auch EBRV 1130 BlgNR XVIII.GP, 140ff

⁵⁸³ *Burgstaller*, Der strafrechtliche Schutz wirtschaftlicher Geheimnisse, 15; *Potyka*, Datenschutz in der Wirtschaft, 131

⁵⁸⁴ *Arnold*, Bankgeheimnis, 8; ebenso *Avancini* in *Avancini/Iro/Koziol*, BVR I, Rz 2/47; *Snizek*, Wie gut ist das österreichische Bankgeheimnis ?, ÖSpz 1987, 174ff

Das Gegenteil vom Geheimnis ist die Offenkundigkeit. Offenkundig ist eine Tatsache dann, die die Sphäre des Alleinwissenden oder der zur Verschwiegenheit verbundenen Gemeinsamwissenden in einer Weise verlassen hat, die es nach praktischer Lebenserfahrung als unwahrscheinlich erscheinen lässt, dass sie sich noch innerhalb eines übersehbaren und feststellbaren Kreises zu ihrer weiteren Geheimhaltung Entschlossener befindet. Eine generelle Begriffsbestimmung von Offenkundigkeit zum Gegenteil von Geheimnis ist jedoch nicht möglich und daher lässt sich kurzerhand zusammengefasst gesagt werden, dass man unter einem Geheimnis Tatsachen versteht, die nur bestimmten Personen bekannt sind und die anderen nicht bekannt werden sollen.⁵⁸⁵

Damit ein Bankberater optimal auf die Bedürfnisse eines Kunden eingehen kann und ihm ein für beide Seiten günstiges Angebot machen will, dann benötigt er Informationen über die finanziellen Verhältnisse und Bedürfnisse des Kunden. Ohne diese Informationen und dem dadurch aufgebauten „Schutzschild“ nach außen wäre eine Geschäftsbeziehung von Seiten des Kunden nicht möglich.

Diese Geheimhaltungsverpflichtung gilt zeitlich und gegenüber jedermann unbegrenzt und daher auch nach Beendigung des Dienstverhältnisses.⁵⁸⁶ Der Kreis der betroffenen Personen, die an das Bankgeheimnis gebunden sind, ist im Gesetz ausdrücklich umschrieben. Die Aufzählung (Kreditinstitute, ihre Gesellschafter, Organmitglieder, Beschäftigte sowie sonst für Kreditinstitute tätige Personen) weist darauf hin, dass dieser Ausdruck im Sinne und dem Zwecke des Gesetzes folgend extensiv auszulegen ist. Daraus ergibt sich weiter, dass wenn Organen von Behörden bei ihrer dienstlichen Tätigkeit Tatsachen bekannt geworden sind, die dem Bankgeheimnis unterliegen, diese in weiterer Folge durch das Amtsgeheimnis geschützt sind.⁵⁸⁷ An sich besteht kein subjektives Recht auf Wahrung des Amtsgeheimnisses.⁵⁸⁸ Im besonderen Fall des zum Amtsgeheimnis transformierten Bankgeheimnisses wird man nach *Avancini*⁵⁸⁹ dem Geheimnisherrn zur Abrundung seines Geheimnisschutzes aber doch einen Anspruch auf Wahrung des Amtsgeheimnisses zuerkennen müssen, und er hat daher auch das Recht, einen Bescheid, durch den ein Organ von der Amtsverschwiegenheit entbunden wird, mit der Begründung anzufechten, es liege keiner der Ausnahmefälle des § 38 Abs 2 BWG vor. Ob aufgrund dieser Ausstrahlung ein subjektives Recht auf Wahrung des

⁵⁸⁵ So *Sichtermann*, Bankgeheimnis und Bankauskunft

⁵⁸⁶ OGH in SZ 57/29; 4 Ob 36/01z in ÖBA 2001, 828; *Laurer* in BWG-Komm § 38 Rz 9

⁵⁸⁷ *W. Ulrich*, in *Ruppe* (Hrsg) Geheimnisschutz im Wirtschaftsleben, 290; *Schinnerer*, Aktuelle Probleme zum Recht des Kreditwesens, (Ö)BWG

⁵⁸⁸ VfGH in VfSlg 3.005; 7.455; B 4/91 in JBl 1992, 382

⁵⁸⁹ In BVR I, Rz 2/59

Amtsgeheimnisses möglich ist⁵⁹⁰, erscheint zweifelhaft weil der einfache Gesetzgeber die Pflicht zur Wahrung des Amtsgeheimnisses zwar einschränken, aber nicht ausdehnen darf.⁵⁹¹ Die Zuerkennung eines subjektiven Rechts auf Wahrung der Amtsverschwiegenheit durch den einfachen Gesetzgeber würde diesem Grundsatz widerstreiten. Außerdem bezieht sich das Recht auf Geheimhaltung nach dem DSG auch auf Daten aus dem Erwerbsleben und über das Unternehmen⁵⁹², sodass hiemit ein Großteil des bankgeheimnisrechtlichen Schutzbereichs abgedeckt ist.⁵⁹³

Keine Amtsverschwiegenheit besteht aufgrund einer verfassungsrechtlichen und damit dem BWG übergeordneten Regelung gegenüber der Volksanwaltschaft, wenn die Tätigkeit des Kreditinstituts der Verwaltung des Bundes oder der Länder zugerechnet werden kann, die nach Art 148 i B-VG die Zuständigkeit für den Bereich der Verwaltung begründet.⁵⁹⁴ Ebenso lässt das BWG die in Verfassungsbestimmungen des Art 126b, 127 und 127a B-VG enthaltenen Auskunftspflichten gegenüber dem Rechnungshof unberührt wenn an einem Kreditinstitut eine entsprechende Beteiligung von Bund, Ländern oder Gemeinden besteht.⁵⁹⁵ Die Verschwiegenheitspflicht der Bank entfällt nur, soweit der Rechnungshof die betreffenden Unterlagen und Auskünfte zur Wahrnehmung seines Auftrages benötigt. Darüber hat er sodann Verschwiegenheit zu bewahren.⁵⁹⁶

Der Begriff „Geschäftsverbindung“ im 1. Satz des § 38 BWG muss (noch) keine vertragliche Verbindung zwischen Kunden und Kreditunternehmung ausdrücken. Es reicht dazu aus, dass dem Kunden für seine Geschäfte die Einrichtungen der Bank zur Verfügung gestellt werden.⁵⁹⁷ Zu beachten ist, dass das DSG 2000 alle Daten – ob sie nun ein Geheimnis enthalten oder nicht – und nicht nur solche aus der Geschäftsverbindung mit Kunden schützt. Sieht das Datenschutzgesetz nun weitergehende Verschwiegenheitspflichten vor, so sind diese zu beachten. Das Bankgeheimnis ist jedoch auch dann zu wahren, wenn eine Weitergabe von Informationen nach dem DSG 2000 iSv § 7ff DSG 2000 zulässig wäre.⁵⁹⁸

⁵⁹⁰ So *Avancini in Avancini/Iro/Koziol*, BVR I (1987), Rz 2/7 und *Apathy in Apathy/Iro/Koziol*, BVR I, Rz 2/58

⁵⁹¹ VfSlg 9657/1983

⁵⁹² VfSlg 12.228/1989 (Wirtschaftsdaten)

⁵⁹³ *Oppitz*, Das Bankgeheimnis, Geheimnisschutz-Datenschutz-Informationsschutz (2008), 279

⁵⁹⁴ *Laurer*, BWG-Komm § 38; *Apathy/Iro/Koziol*, BVR I, 255, Rz 2/60

⁵⁹⁵ *Laurer*, Handkommentar, Rz 14 zu § 23 KWG

⁵⁹⁶ Vgl § 12 Abs 5, § 15 Abs 2, § 18 Abs 2 RHG

⁵⁹⁷ *Schinnerer*, Aktuelle Probleme zum Recht des Kreditwesens, Schriftenreihe (Ö)BWG, 179 – zu § 23 KWG

⁵⁹⁸ *Weiss*, Bankgeheimnis und Datengeheimnis, EDVuR 1994, 86; *Laurer* spricht auch von einem „Kummulationsgebot“, Handkommentar zum KWG, 9ff

Die Ermittlung und Verarbeitung von Kunden- und Geschäftsbeziehungsdaten wie zB Einkommen, Höhe und Laufzeit von Krediten und deren Besicherung und Ausnutzung, allfällige Nichteinhaltung von finanziellen Verpflichtungen, Wert und Zusammensetzung von Wertpapierdepots, Kontostandsinformationen, missbräuchliche Verwendung von Bankomat- und/oder Kreditkarte(n) gehören zum berechtigten Zweck von Kreditunternehmungen im Rahmen der jeweiligen Tätigkeit iSd § 1 BWG und beinhalten wesentliche Informationen über die Kreditwürdigkeit der Betroffenen. Durch Er- und Übermittlung der inskribierten Daten durch eine Kreditunternehmung an eine zentrale Stelle, die selbst der Geheimhaltung unterliegt, kann keine Interessenbeeinträchtigung gesehen werden. Weiters treten Informationen über die wirtschaftlichen Verhältnisse eines Kreditnehmers oder eines Anlagekunden hinzu.⁵⁹⁹

Nachdem sich der Anwendungsbereich des Bankgeheimnisses auf Kreditinstitute beschränkt hat der Gesetzgeber in Bezug auf Wertpapierdienstleistungsunternehmen im der der WAG-Novelle 2001⁶⁰⁰ ein dem § 38 BWG nachgebildetes Berufsgeheimnis für Handelnde auf den Kapitalmärkten geschaffen. Im Unterschied zur Bestimmung des § 38 Abs 1 BWG ist anzumerken, dass das Berufsgeheimnis nach § 7 WAG⁶⁰¹ (vormals § 21a WAG) nicht auf Gesellschafter, Organmitglieder sowie sonst für das Wertpapierunternehmen tätige Personen erstreckt wurde. Der Schutz gilt jedoch nur wenn es zu einem Abschluss eines Wertpapiergeschäftes kommt. Offenbart ein Kunde seine Vermögensverhältnisse zB im Rahmen eines Beratungsgespräches so gilt der Schutz des Berufsgeheimnisses nicht. Ebenso wenig im Zeitraum zwischen Offenbarung des Geheimnisses und der tatsächlichen Ausführung des Wertpapiergeschäftes.⁶⁰² In Anlehnung an § 38 BWG wurde im Gegensatz zur Vorgängerregelung des § 21 WAG, die Zustimmung zur Offenbarung von Geheimnissen auch auf „ausdrücklich und schriftlich“ erstreckt.

⁵⁹⁹ Ulrich, Überlegungen zum Bankgeheimnis, in: *Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben (1980) 283, 287; vgl dazu auch die Nachforschungspflichten nach § 13 Z 3 WAG

⁶⁰⁰ BGBl 2001/97

⁶⁰¹ § 7 WAG lautet: (1) Wertpapierfirmen und Wertpapierdienstleistungsunternehmen sowie die für sie tätigen Personen sind zur Verschwiegenheit über Geheimnisse verpflichtet, die sie ausschließlich aus Wertpapiergeschäftes (§ 1 Abs. 1 Z 7 lit. b bis f BWG) oder Wertpapierdienstleistungen gemäß § 3 Abs. 2 ihrer Kunden, die sie im Auftrag ihrer Kunden gemäß § 3 Abs. 2 Z 3 vermitteln oder im Rahmen ihrer Vollmacht gemäß § 3 Abs. 2 Z 2 für diese ausführen, erfahren haben, sofern dieser Verschwiegenheitspflicht keine gesetzliche Auskunftspflicht entgegensteht oder der Kunde der Offenbarung des Geheimnisses schriftlich zustimmt. Die Verschwiegenheitspflicht nach dem ersten Satz gilt weiters nicht, soweit die Offenbarung des Geheimnisses zur Klärung von Rechtsangelegenheiten aus dem Verhältnis zwischen Wertpapierfirmen oder Wertpapierdienstleistungsunternehmen und Kunden erforderlich ist.

(2) ..

⁶⁰² Ausführlich Brandl/Wolfbauer, Finanzdienstleistungen nach dem Finanzmarktaufsichtsgesetz (2001), 61ff

Weiters weist das Bankgeheimnis auch sachliche Überschneidungen mit den Insiderverboten iSd § 48a Abs 1 Z 1 BörseG in deren Sanktionsbereich nicht nur Kreditinstitute und deren Mitarbeiter erfasst sind.⁶⁰³ Die Insiderverbote sind durch die Insider RL 89/592/EWG sowie durch die Marktmissbrauchs RL 2003/6/EG geprägt, jedoch nicht verfassungsrechtlich abgesichert. Sie ist ebenfalls justizstrafrechtlich durch § 48b Abs 1 BörseG abgesichert.⁶⁰⁴

Natürlich stellt sich auch die Frage nach dem Verhältnis der schutzwürdigen Interessen des Betroffenen im Verhältnis zum Schutzbedürfnis bzw. der überwiegenden Interessen des Auftraggebers/Kreditunternehmens. Bei Vertragsbruch durch den Betroffenen sei es durch Nichtbezahlung von Raten oder missbräuchlicher Verwendung von Bankomat- und /oder Kreditkarte(n) wird die jeweilige Person natürlich das Interesse haben, dass diese Informationen nicht über den unmittelbar berührten Personenkreis hinaus bekannt werden, sodass Dritte diese Daten nicht ermitteln und verwenden dürfen.

Ich schließe mich hier der Meinung von *Potyka*⁶⁰⁵ an, dass gerade bei Vertragsbruch oder strafbaren Handlungen iSd StGB, die Schutzwürdigkeit des Vertragsbrüchigen bzw. Täters dem gegenüber zu verneinen ist, der gerade im Begriff ist, das gleiche Vertragsverhältnis einzugehen bzw. der Gefahr durch die gleiche strafbare Handlung geschädigt zu werden, ausgesetzt ist.

Aufgrund des Schutzzweck der Norm ergibt sich, dass damit verhindert werden soll dass Bankgeheimnisse an Dritte offenbart werden und die berechtigten Interessen des Kunden an der Geheimhaltung von Tatsachen, die dem Kreditinstitut im Rahmen der Geschäftsverbindung zur Kenntnis kommen, gewahrt bleiben. Dazu gehört auch, dass bei Tod des Bankkunden, der Bankangestellte dem Verlassenschaftskurator jederzeit zur Auskunft über den Stand der Konten oder Details der Geschäftsbeziehung verpflichtet ist. Ebenso kommt bis zur Einantwortung dem ruhenden Nachlass und dessen Vertreter, also den Erben nach Abgabe der Erbantrittserklärung und hinreichendem Ausweis des Erbrechts (§ 810 ABGB) oder dem Verlassenschaftskurator die Stellung eines Bankkunden zu.⁶⁰⁶ Gesetzliche

⁶⁰³ § 48a Z 1 BörseG (Auszug) lautet: „Insider-Information“ ist eine öffentlich nicht bekannte, genaue Information, die direkt oder indirekt einen oder mehrere Emittenten von Finanzinstrumenten oder ein oder mehrere Finanzinstrumente betrifft und die, wenn sie öffentlich bekannt würde, geeignet wäre, den Kurs dieser Finanzinstrumente oder den Kurs sich darauf beziehender derivativer Finanzinstrumente erheblich zu beeinflussen, weil sie ein verständiger Anleger wahrscheinlich als Teil der Grundlage seiner Anlageentscheidungen nutzen würde.

⁶⁰⁴ *Oppitz*, Bankgeheimnis, Geheimnisschutz-Datenschutz-Informationsschutz, 273ff

⁶⁰⁵ *Potyka*, Datenschutz in der Wirtschaft, Datenschutz im Kreditwesen, 128; ebenso *Pruckner*, Datenschutz im Kreditwesen, 146

⁶⁰⁶ OGH 21.12.1993, 1 Ob 609/93, wbl, 1994, 242; OGH 15.5.1996, 7 Ob 610/95, RdW 1996, 521; ÖBA 2001, 828; *Sailer* in KBB § 810 Rz 1 ff; *Apathy/Iro/Koziol*, 244, 2/42

Vertreter wie Eltern, Vormund, Kurator, Sachwalter eines Kunden sind im Rahmen des ihnen durch das Gesetz oder durch das PflEGschaftsgericht übertragenen vermögensrechtlichen Wirkungsbereiches auskunftsberechtigt.⁶⁰⁷ Ein Noterbe oder Legatar hat hingegen kein Recht, vom Kreditinstitut Auskunft zu verlangen.⁶⁰⁸

Eine bankinterne Weitergabe von Daten an andere Abteilungen, zB von der Privatkundenabteilung an eine eigene Kreditprüfstelle um die Bonität überprüfen zu können, ist im Rahmen einer Interessensabwägung zulässig.⁶⁰⁹

Auch Tatsachen des Giroverkehrs sind Gegenstand des Bankgeheimnisses, soweit es sich nicht um die zur technischen Abwicklung von Überweisungen unvermeidlichen Offenbarungen an (bestimmte) Dritte handelt, denen der Kunde durch die Auftragserteilung konkludent zustimmt. Soweit es bei der Durchführung von Überweisungen notwendigerweise zu einer Offenbarung von Geheimnissen kommen muss, fehlt es an einem objektiven Geheimhaltungsinteresse. Aus objektiver Sicht besteht jedenfalls an der Tatsache, welche Zahlungen ein Bankkunde über seine Bank an Dritte leistet, in der Regel ein Geheimhaltungsanspruch, weil niemand Einzelheiten seiner finanziellen Umstände einem größeren Personenkreis offen zu legen pflegt.⁶¹⁰

Die Kreditunternehmung ist jedoch bei der Feststellung des Vorliegens eines Geschäfts- und Betriebsgeheimnisses mit eigenem berechtigtem Interesse zur Interessensabwägung verpflichtet. Dh der Geheimhaltungsanspruch eines Kunden besteht insoweit nicht, als die Kreditunternehmung zur Wahrung ihrer Rechte gegenüber dem Kunden staatliche Rechtspflege in Anspruch nehmen muss (durch Einbringung einer Klage oder Erstattung einer Strafanzeige) und damit zur Offenbarung von Tatsachen über diesen Kunden gezwungen ist.⁶¹¹ Ähnliches gilt wenn das Kreditinstitut zur Hereinbringung einer Forderung ein Inkassobüro einschaltet und dadurch bankgeheimnisrechtliche Tatsachen übermittelt. Mithilfe der Rechtsfigur des „internen Bankgeheimnisses“ (siehe dazu unten Seite 256) sind die zu übermittelnden Informationen auf das Notwendigste zu beschränken.⁶¹² Einer anderen Meinung die Datenübermittlung an ein Gericht als Notwehr-/Nothilfehandlung zu rechtfertigen kann in meinen Augen nicht gefolgt werden.⁶¹³

⁶⁰⁷ OGH in SZ 43/67; *Schinnerer/Avancinci* I, 192; *Apathy/Iro/Koziol*, 243, Rz 2/37

⁶⁰⁸ *Apathy/Iro/Koziol*, 245, Rz 2/42

⁶⁰⁹ *Ungnade*, Datenschutz m Kreditgewerbe, 90

⁶¹⁰ OGH 25.2.1992, 4 Ob 114/91, EvBl 1992/58 – ergangen zu § 23 KWG

⁶¹¹ *Potyka*, in Datenschutz in der Wirtschaft, Datenschutz im Kreditwesen, 132; so auch *Burgstaller*, Der strafrechtliche Schutz, 16

⁶¹² *Jabornegg*, Neues zum Bankgeheimnis, WBl 1990, 29, 57ff sowie ihm folgend *Apathy* in *Apathy/Iro/Koziol*, BVR I, Rz 2/21

⁶¹³ So *Haushofer-Schinnerer-Ulrich*, Die österreichischen Kreditwesengesetze, 81; ebenfalls bejahend *Weissel*, Die Negativliste der Banken aus datenschutzrechtlicher Sicht, EDVuR 1990,62

Die Bestimmungen des BWG über das Bankgeheimnis und des DSG sind kumulativ anzuwenden und bestehen nebeneinander.⁶¹⁴ Gemäß § 15 Abs 1 DSG 2000 werden bestehende Verschwiegenheitspflichten durch die Zulässigkeit von Übermittlungen gemäß § 7 Abs 2 DSG 2000 nicht berührt; trotz Zulässigkeit der Übermittlung nach § 7 ff DSG 2000 darf diese also nicht erfolgen, wenn eine gesetzliche Verschwiegenheitspflicht besteht.⁶¹⁵ Wenn daher sowohl ein dem DSG unterliegendes "Übermitteln" als auch ein Eingriff in das Bankgeheimnis vorliegt, sind die (einander teilweise überschneidenden) Einschränkungen des DSG und des BWG zu wahren; insbesondere unterliegen dem DSG auch Daten, die an sich überhaupt keinen Geheimnischarakter haben.

Bei § 38 Abs 1 BWG handelt es sich um einen Fall des Berufsgeheimnisses und berechtigt daher den Bankangestellten auch im Zusammenhang einer Zeugenaussage in einem Finanzstrafverfahren zur Verschwiegenheit iSd § 104 Abs 1 lit d FinStrG.

Eine Entbindung vom Bankgeheimnis kann nur ausdrücklich und schriftlich erfolgen (§ 38 Abs 2 Z 5 BWG), nicht jedoch aufgrund von AGB's, die nicht unterschrieben werden.⁶¹⁶

Auch bei einem Gemeinschaftskonto, über welches jeder Kontoinhaber einzelverfügungsberechtigt ist, ist das Einverständnis sämtlicher Kontoinhaber einzuholen, denn die Zustimmung zur Erteilung einer Auskunft ist keine Verfügung über das Konto im engeren Sinn.⁶¹⁷

Wie bei Geschäfts- und Betriebsgeheimnissen besteht hier die Bedeutung des Geheimhaltungswillen „im Negativen“⁶¹⁸: Die Kreditunternehmung hat grundsätzlich von einem allumfassenden Geheimhaltungswillen der betroffenen Personen auszugehen. Auf diesen Willen kann – trotz der Bestimmung des § 38 Abs 2 Z 5 BWG – nicht nur ausdrücklich, sondern auch konkludent verzichtet werden. So sind zB Daten davon ausgenommen, die die Durchführung eines Kundenauftrages ohne entsprechende Weitergabe von Kundendaten, unmöglich machen würden. (zB im Rahmen eines Überweisungsauftrages)

⁶¹⁴ *Duschanek/Rosenmayr-Klemenz*, DSG 2000, § 15 Z 3

⁶¹⁵ Für Berufsgruppen welche durch ein eigenes Ständerecht gekennzeichnet sind wie etwa Rechtsanwälte und Wirtschaftstreuhänder liegt daher eine Verdopplung der Geheimhaltungspflicht vor; siehe dazu auch *Apathy/Iro/Koziol*, BVR I, Rz 2/19

⁶¹⁶ VwGH 20.2.1992, 90/16/0156; OGH 19.11.2002 4 Ob 179/02 f; *Iro*, OGH: Unwirksame Klauseln in den Allgemeinen Geschäftsbedingungen der Banken, RdW 2003, 66; *Graf*, Jetzt schlägts aber (fast) 13 ! – Geschäftsbedingungen der Kreditinstitute: OGH erklärt 12 Klauseln der Banken AGB 2000 für unwirksam, ecolex Skript Nr 24, ecolex 2003 H 2

⁶¹⁷ Vgl *Iro* in BVR, Rz 4/85 ff

⁶¹⁸ *Burgstaller*, Der strafrechtliche Schutz, 15

Abschließend kann festgestellt werden, dass die zum berechtigten Zweck einer Kreditunternehmung gehörenden Übermittlungen bedeuten unter der Zugrundelegung des oben angeführten Geheimnisbegriffes auch keine Verletzung des Bankgeheimnisses, da es entweder am Geheimhaltungswillen des Berechtigten oder am Vorliegen eines berechtigten Geheimhaltungsinteresses mangelt.

Das Bankgeheimnis gilt nicht (§ 38 Abs 2 BWG)

1. im Zusammenhang mit einem Strafverfahren⁶¹⁹ auf Grund einer gerichtlichen Bewilligung (§ 116 StPO) gegenüber den Staatsanwaltschaften und Strafgerichten und mit eingeleiteten Strafverfahren wegen vorsätzlicher Finanzvergehen, ausgenommen Finanzordnungswidrigkeiten, gegenüber den Finanzstraßbehörden;
2. im Falle der Verpflichtung zur Auskunftserteilung nach § 41 Abs. 1 und 2 BWG (Geldwäße und Terrorismusfinanzierung), § 61 Abs. 1 BWG (Bankprüfer), § 93 und § 93a BWG (Einlagensicherung und Anlegerentschädigung);
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;
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.

Ob der o.a. Katalog eine *taxative* Aufzählung beinhaltet ist str. Sowohl die hL⁶²⁰ als auch der VwGH⁶²¹ und der OGH⁶²² teilt die Meinung, dass weitere Ausnahmen möglich sind weil der Gesetzgeber auch an anderer Stelle – ohne Ergänzung des Katalogs des § 38 Abs 2 BWG – etabliert. (siehe § 5 Abs 3 und § 6 Abs 8 DevisenG 2004).

Eine weitere Ausnahme nach hL und Rechtsprechung liegt in der Anerkennung des Vorranges der exekutionsrechtlichen Auskunftspflicht nach § 301 EO, wenn der Drittschuldner ein

⁶¹⁹ Ein parlamentarischer Untersuchungsausschuss ist kein Strafgericht und daher ist der Durchbrechungstatbestand nicht anwendbar; siehe dazu auch *Flora*, Das Bankgeheimnis im gerichtlichen Strafverfahren (2007)

⁶²⁰ Vgl die Nachweise bei *Apathy* in *Apathy/Iro/Koziol*, Österreichisches Bankvertragsrecht I (2007), Rz 2/62

⁶²¹ VwGH 94/17/0297 vom 28.10.1994, ÖBA 1995, 641

⁶²² ÖBA 1988,1022 mit Anm *Jabornegg* wo eine Kreditkartengesellschaft einem Vertragsunternehmen auf dessen Verlagen die Privatadresse eines Kreditkarteninhabers bekannt gegeben hat weil es zu einer Störung der Geschäftsabwicklung kam

Kreditinstitut ist.⁶²³ Für die Durchbrechung des Bankgeheimnisses spricht die Tatsache, dass der betreibende Gläubiger in gewisser Weise in die Stellung des Kunden einrückt und insoweit auch dessen Auskunftsanspruch geltend macht.⁶²⁴

Als Ausnahme vom Bankgeheimnis kann auch die vom OGH entwickelte Lösung in Bezug auf die Informationspflicht des Gläubigers beim Abschluss eines Bürgschaftsvertrages bzw. Pfandvertrages gesehen werden. Eine Bank ist grundsätzlich nicht verpflichtet, einen Bürgen vor dem Abschluss eines Bürgschaftsvertrages über die Vermögensverhältnisse des Schuldners aufzuklären. Dies gilt auch für die selbstschuldnerische Bürgschaft⁶²⁵ als auch den Pfandvertrag.⁶²⁶

Hat der Bürge grundsätzlich seine wirtschaftlichen Interessen selbst zu wahren, kann er auch von der Bank eine Aufklärung darüber nicht erwarten, ob das Ausmaß der nach der von der Bank gewählten Vertragsgestaltung klaren Bürgschaftsverpflichtung seine wirtschaftliche Leistungsfähigkeit übersteigt.

Eine Warnpflicht einer kreditgewährenden Bank gegenüber dem Bürgen ist aber dann anzunehmen, wenn die Bank schon Kenntnis von der Zahlungsunfähigkeit oder einem unmittelbar bevorstehenden wirtschaftlichen Zusammenbruch des Kreditnehmers hat und diesem gerade wegen der vom Dritten geleisteten Sicherheit trotzdem noch einen Kredit gewährt. Das Wesen der Bürgschaft besteht jedoch in der Sicherstellung einer Schuld⁶²⁷, sodass es für den Bürgen in der Regel ohne Bedeutung ist, ob die Schuld, für die er sich verbürgt, bereits besteht oder unmittelbar mit der Bürgschaftsübernahme begründet wird. Der besondere Wissensstand der Bank kann überdies durch den Umstand aufgewogen werden, dass der dem Hauptschuldner "eingeräumte" Kredit gar nicht zu dessen wirtschaftlicher Verfügung bestimmt war und die Bürgschaft lediglich zur Sicherstellung eines bereits Not leidend gewordenen Kredites bestimmt war. Zweck eines Kredites ist, dem Kreditnehmer Bargeld oder ein entsprechendes Surrogat zu verschaffen. Dient aber der „eingeräumte“ Kredit nicht diesem Zweck, sondern lediglich dazu eine bereits eingeräumte Überziehungsmöglichkeit und demnach bereits gewährten Kredit urkundlich festzuhalten, so

⁶²³ Siehe hiezu die Nachweise bei *Apathy*, Abtretung von Bankforderungen und Bankgeheimnis, ÖBA 2006, 33, 35 Fn 48 sowie *Jabornegg-Strasser-Floretta*, Das Bankgeheimnis, 155; *Apathy/Iro/Koziol*, BVR I, 306, FN 608; *Riefel*, Drittschuldneräußerung von Kreditunternehmen im Hinblick auf das Bankgeheimnis, QuHGZ 1/1981, 163ff; *Arnold*, Bankgeheimnis, 22ff; gegen eine Derogation der bankgeheimnisrechtlichen Vorschriften jedoch SZ 57/29

⁶²⁴ *Jabornegg/Strasser-Floretta*, Bankgeheimnis 154ff; *Jabornegg*, ÖBA 1997, 673; ebenso zum Pfandgläubiger *Jabornegg*, ÖBA 1992, 660

⁶²⁵ OGH 7.11.1985, 7 Ob 625/85, EvBl.1984/160; SZ 56/81).

⁶²⁶ SZ 53/153; EvBl 1983/128, 184/90, 1984/160; Steiner, Zur Aufklärungspflicht einer Kreditunternehmung bei Wechselgeschäften, JBl 1983, 189ff; OGH 11.4.1985, 3 Ob 629/83 unter Bezugnahme auf § 1369 ABGB

⁶²⁷ *Koziol-Welser*, Grundriss I, 279

ist eine Warnpflicht der Bank auch unter diesen Voraussetzungen in einem solchen Fall gegeben.

Obwohl ein Gläubiger auch nicht den Pfandgläubiger/Bürgen benachrichtigen muss wenn dieser kurz vor Zahlungsunfähigkeit steht, so ist trotzdem der Meinung beizupflichten, dass wenn er die begründete Besorgnis hat, dass der Hauptschuldner zahlungsunfähig wird oder im Begriff ist sich ins Ausland abzusetzen und ihm auch bekannt ist, dass der Pfandgläubiger/Bürge dieses Wissen dezidiert nicht besitzt, dann muss er aufgrund der Sorgfaltspflichten diesen darüber informieren. Eigene Nachforschungen braucht der Gläubiger aber nicht anzustellen.⁶²⁸

Eine Verletzung dieser Aufklärungspflichten kann zu Schadenersatz oder bei Arglist auch zur Anfechtung des Pfandvertrages/Bürgschaftsvertrages führen.⁶²⁹

Weiters kann gesagt werden, dass wenn eine Bürgschaft/Pfandvertrag mit (auch formloser) Einwilligung des Hauptschuldners übernommen wurde und er keine Vorbehalte bezüglich Auskunftserteilung an den Bürgen/Pfandbesteller gemacht hat, die Bank von der Einhaltung des Bankgeheimnisses (und der Geheimhaltung nach dem DSG) in dem Umfang auch soweit entbunden ist, als der Pfandbesteller/Bürge gesetzliche Auskunftsansprüche hat, wie sie ihm auch zustünden, wäre der Gläubiger keine Kreditunternehmung.

Nach Bezahlung der Forderung durch den Bürgen/Pfandbesteller setzt sich der Auskunftsanspruch nach § 1358 ABGB gegenüber dem Bankgeheimnis durch weil das Interesse des Gläubigers an einem Regress zweifellos bei weitem das Interesse des Hauptschuldners an Geheimhaltung überwiegt. Die Zahlung bringt die Forderung nicht zum Erlöschen, sondern sie bewirkt ipso iure deren Übergang auf den Zahler. Dieser kann sodann gemäß § 1358 Satz 2 ABGB vom Gläubiger die Herausgabe der vorhandenen Rechtsbehelfe und Sicherungsmittel verlangen.⁶³⁰

Gemäß § 38 Abs 2 Z 5 BWG hat die Entbindung vom Bankgeheimnis "ausdrücklich" und "schriftlich" zu erfolgen. Der Senat hat erst vor kurzem in seiner Entscheidung⁶³¹ ausgesprochen, dass die Aufnahme der Klausel in - regelmäßig nicht unterfertigte -

⁶²⁸ *Ohmeyer*, ZBl 1927, 171

⁶²⁹ Vgl JBl, 1981, 425 mwN

⁶³⁰ So auch OGH 2.2.1984, EvBl 1984/90 = JBl 1984, 614; *Avancini*, Der Auskunftsanspruch des Bürgen gegenüber dem Gläubiger – zugleich ein Beitrag zum Bankgeheimnis, JBl 1985, 193; auf weitere Details muss aufgrund fallspezifischer Literatur und damit verbundener Umfassendheit verzichtet werden; ebenso SZ 57/29, ÖBA 1992, 654 mit Anm *Jabornež*, *Apathy/Iro/Koziol*, BVR I, 301, Rz 2/133

⁶³¹ OGH 4 Ob 28/01y (ÖBA 2001, 645 = *ecolex* 2001/147)

Allgemeine Geschäftsbedingungen nicht für eine (wirksame) Entbindung vom Bankgeheimnis ausreiche.⁶³²

Dies wird in der Lehre⁶³³ auch zutreffend dahin verstanden, dass die bloße Unterfertigung von Unterschriftsprobenblättern, in denen auf die Geltung der Allgemeinen Geschäftsbedingungen hingewiesen wird, für eine rechtsgültige Vereinbarung nicht ausreicht und die entsprechende Vereinbarung durch Unterfertigung des Vertragsformblattes selbst zu erfolgen hat. Es besteht daher kein Anlass, von der in 4 Ob 28/01y⁶³⁴ vertretenen Auffassung abzuweichen. Danach bedeutet das Gebot der Schriftlichkeit, dass der Kunde das die Zustimmungserklärung enthaltende Schriftstück unterfertigen muss. Die geforderte Ausdrücklichkeit bedingt, dass die Entbindungserklärung klar und deutlich im unterfertigten Schriftstück enthalten ist.⁶³⁵ Angesichts der besonderen Bedeutung des Bankgeheimnisses muss nämlich sichergestellt sein, dass auch ein Kunde, der das Schriftstück nur oberflächlich studiert, die Entbindungserklärung zur Kenntnis nimmt und sie im Bewusstsein ihrer Bedeutung unterzeichnet.

Dies ist aber dann nicht der Fall, wenn die Entbindungserklärung in dem vom Kunden unterfertigten Vertragsformblatt nicht abgedruckt ist, zumal die Geschäftsbedingungen in aller Regel nicht unterfertigt werden. Die Aufnahme der Klausel in die vom Kunden ohnehin zu unterfertigenden Vertragsformblätter erspare die als unmöglich angesehene Unterfertigung der Allgemeinen Vertragsbedingungen.

Da § 38 BWG keine Widerrufsmöglichkeit für die einmal abgegebene Zustimmungserklärung enthält, ist in der Informationsweitergabe an Dritte nach erfolgter ausdrücklicher schriftlicher Zustimmung des Betroffenen trotz späteren Widerrufs keine Verletzung des Bankgeheimnisses zu sehen. (natürlich ist die Entbindung vom Bankgeheimnis grundsätzlich widerrufbar⁶³⁶) Es kann daher zu einem Auseinanderfallen der Zulässigkeit der Übermittlung nach § 8 Abs 1 Z 2 DSG 2000 und § 38 Abs 2 Z 5 BWG kommen. Dass die Beachtlichkeit des Widerrufs nach DSG 2000 nicht zwingend zur Unzulässigkeit der Datenübermittlung führt, ergibt sich daraus, dass § 8 DSG 2000 auch andere Zulässigkeitsbedingungen nennt.⁶³⁷

⁶³² So bereits schon *Pruckner*, Datenschutz im Kreditwesen, 147 und *Stadler*, ÖZW 1979,15; aA hingegen *Duschanek*, Datenschutzgesetz, 44

⁶³³ *Rabl* zu ecolex 2001/147

⁶³⁴ OGH 22.3.2001, 4 Ob 28/01y

⁶³⁵ ÖBA 1997, 632

⁶³⁶ OGH 7 Ob 2299/96f in ÖBA 1997, 632

⁶³⁷ So auch *Potyka*, in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, Datenschutz im Kreditwesen, 135

Noch kurz eingehen möchte ich auf die von Lehre und Rsp entwickelte Figur des „*internen Bankgeheimnisses*“⁶³⁸. Der Geheimhaltungsanspruch des Kunden wird schon dadurch verletzt, dass eine geheim zu haltende Tatsache innerhalb derselben Bank an Personen bekannt gegeben wird, die mit der Sache des Kunden in keiner Weise befasst sind und der Kunde auch innerhalb der Organisation eine vertrauliche Behandlung seiner Angelegenheiten erwarten darf⁶³⁹. Der Unterschied zwischen insiderrechtlichen „Compliance“-Vorschriften und dem „internen Bankgeheimnis“ liegt in der Motivation des Geheimnisschutzes: Beim Insiderrecht geht es um die Verhinderung der missbräuchlichen Ausnützung kurssensibler Informationen vor allen anderen wogegen es beim internen Bankgeheimnis um den dem Persönlichkeitsschutz nahe stehende Eigenschaft der Sicherheit des Bankkunden geht, keine Informationen zu seiner persönlichen Vermögenssituation in unkontrollierbarer Form in sämtlichen Geschäftsbereichen eines Kreditinstituts auswerten zu lassen. Das Selbstbestimmungsrecht des Kunden soll auch in Bezug auf die Betreuungsintensität gewahrt bleiben.⁶⁴⁰

Verstöße gegen das Bankgeheimnis werden nach § 101 Abs 1 BWG vom Gericht mit Freiheitsstrafen bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen geahndet wenn jemand Tatsachen des Bankgeheimnisses offenbart oder verwertet, um sich oder einem anderen einen Vermögensvorteil zu verschaffen oder um einem anderen einen Nachteil zu zufügen. Nur eine nach § 38 Abs 1 BWG geheimhaltungspflichtige natürliche Person kann die Tat begehen. Außenstehende können sich jedoch als Beteiligte iSd § 12 StGB strafbar machen⁶⁴¹.

Der Täter ist jedoch nur auf Antrag des Geschädigten zu verfolgen. Seit dem 1. Oktober 1993 ist nicht mehr der Einzelrichter des Gerichtshofes I. Instanz zuständig, sondern das Bezirksgericht. (§ 30 StPO)

Die FMA ist als Aufsichtsbehörde auch berechtigt Bankgeheimnisverletzungen zu ahnden. Hiezu steht ihr unter Androhung einer Zwangsstrafe der Katalog der aufsichtsrechtlichen Maßnahmen nach § 70 Abs 4 BWG zur Verfügung an deren unterster Stelle die Wiederherstellung des rechtmäßigen Zustandes steht welcher im Hinblick auf die Umstände des Falles angemessen ist. (Z1) Der Maximalbetrag einer derartigen Zwangsstrafe beträgt € 20.000 (vgl § 96 BWG). Im Wiederholungsfalle hat die FMA gemäß § 70 Abs 4 Z 2 BWG

⁶³⁸ OGH 25.2.1992, 4 Ob 114/91, ÖBA 1992, 829 mit Anm *Jabornegg*; *Borns*, Das österreichische Bankrecht-systematische Darstellung des BWG², 285 Fn 7; *Apathy* in *Apathy/Iro/Koziol*, Österreichisches Bankvertragsrecht I (2007), Rz 2/54

⁶³⁹ ÖBA 1992, 829ff mit Anm *Jabornegg*, 837

⁶⁴⁰ *Oppitz*, Das Bankgeheimnis in Geheimnisschutz-Datenschutz-Informationsschutz (2008), 275; FN 463

⁶⁴¹ Vgl *Arnold*, ZGV-Service 1981/1, 21; *Laurer* in BWG-Komm § 101 Rz 1

den Geschäftsleitern des Kreditinstituts die Geschäftsführung ganz oder teilweise zu untersagen. Kann die Funktionsfähigkeit des Kreditinstituts überhaupt nicht mehr sichergestellt werden, so ist auch eine Zurücknahme der Konzession iSv § 70 Abs 4 Z 3 BWG vorgesehen.⁶⁴²

Die Verletzung des Bankgeheimnisses kann gerichtlich auch noch nach

- § 51 DSG („Weiterleitung geheimer Daten“)
- § 11 Abs 1 UWG („Weiterleitung von geheimen Informationen zu Zwecken des Wettbewerbes“)
- § 310 StGB („Verletzung des Amtsgeheimnisses“) sowie
- § 252 FinStrG für Organe der Abgabenbehörde

verfolgt werden.

Dem Bankkunden kommt jedenfalls die Gehilfenhaftungsbestimmung des § 1313a ABGB zugute, sodass dem Kreditinstitut die rechtswidrige Weitergabe von geheimen Informationen durch Mitarbeiter zu zurechnen ist. § 33 Abs 2 DSG 2000 verschärft diese Haftung auch noch durch eine „Leutehaftung“ welche über die Bestimmungen des § 1313a ABGB hinausgeht.⁶⁴³

Die aus der Geschäftsverbindung zwischen Kreditinstitut und Geheimnisherrn entstandenen vertraglichen Pflichten treffen den dort tätigen Mitarbeiter grundsätzlich nicht persönlich wobei für das Kreditinstitut der erhöhte Sorgfaltsmaßstab des § 1299 ABGB maßgeblich ist.⁶⁴⁴ Auch die vertragliche Beziehung zwischen dem Mitarbeiter und dem Kreditinstitut entfaltet keine Schutzwirkung zugunsten des Bankkunden, die den Mitarbeiter dem Bankkunden gegenüber vertraglich haftbar machen würde. Dh eine Geheimhaltungsverpflichtung des Mitarbeiters gegenüber dem Bankkunden besteht nicht. (und daher auch keine Anwendbarkeit der Beweislastumkehr nach § 1298 ABGB)⁶⁴⁵

Grundsätzlich genügt zur Begründung der Haftpflicht leichte Fahrlässigkeit. *Jabornegg/Strasser/Floretta*⁶⁴⁶ sehen jedoch einen zwingenden Charakter in § 23 KWG (jetzt § 38 BWG), der die Haftung für Verletzungen des Bankgeheimnisses auch vertraglich nicht vom Vorliegen groben Verschuldens abhängig machen könne. § 38 BWG schreibt jedoch nur

⁶⁴² *Apathy/Iro/Koziol*, BVR I, 323, Rz 2/168

⁶⁴³ *Koziol*, Haftpflichtrecht II², 202ff

⁶⁴⁴ *Apathy/Iro/Koziol*, BVR I, 316, Rz 2/156

⁶⁴⁵ *Schobel*, Auskunftshaftung, Vertragsfiktionen und Eigenhaftung des Gehilfen, ÖBA 2001, 752 [757]; *Koziol*, Haftpflichtrecht I³, Rz 16/40 mwN

⁶⁴⁶ *Diesselben*, Bankgeheimnis, 163

die Geheimhaltungspflicht fest und sagt nichts über die Haftungsfolgen bei dessen Verletzung aus. Diese Folgen werden durch die dispositiven Bestimmungen der §§ 1295ff ABGB festgeschrieben.

Der zwingende Charakter der Geheimhaltungspflicht ist auch durch die Bestimmungen des

- § 38 ABS 2 Z 5 BWG - Zustimmung zur Geheimnisoffenbarung durch den Kunden und
- § 38 Abs 2 Z 6 BWG - Erteilung einer allgemein gehaltenen banküblichen Auskunft über Unternehmen

offensichtlich zu verneinen. Die Haftung für leichte Fahrlässigkeit kann daher grundsätzlich vertraglich abbedungen werden.⁶⁴⁷ Eine Schadenersatzpflicht tritt dann nur bei grobem Verschulden ein. Nicht beschränkt werden dadurch aber Unterlassungs-, Beseitigungs- und Bereicherungsansprüche des Geheimnisherrn, da diese ja verschuldensunabhängig sind und keinen Schadenseintritt voraussetzen.⁶⁴⁸ Der Unterlassungsanspruch kann nach §§ 378, 381 EO auch durch eine einstweilige Verfügung gesichert werden⁶⁴⁹; Sicherungsmittel ist ein Verbot gemäß § 382 Z 5 EO.

Bei Vorliegen der Haftungsvoraussetzungen gebührt dem „verletzten“ Geheimnisträger (Schädigung unter Kaufleuten) grundsätzlich neben dem positiven Schaden auch der Ersatz des entgangenen Gewinns.⁶⁵⁰ Aufgrund der Gesetzesmaterialien zu § 1328a ABGB besteht grundsätzlich kein Ersatz für ideelle Schäden durch Geldleistung bei Verletzung des Bankgeheimnisses, sondern allenfalls Naturalrestitution.⁶⁵¹ (insbesondere auch bei Rufschädigung [§ 1330 ABGB])

Kreditinstitut Mitarbeiter haben jedoch nur für den positiven Schaden aufzukommen; der entgangene Gewinn ist nur bei grobem Verschulden zu ersetzen (§§ 1323, 1324 ABGB)⁶⁵²

⁶⁴⁷ Schobel, Verletzung von Geheimhaltungspflichten durch Banken, ÖBA 2004, 8; siehe auch ABB Z 9

⁶⁴⁸ Koziol, Haftpflichtrecht I, Rz 2/1

⁶⁴⁹ Kodek in Angst, EO-Komm § 378 Rz 8 und § 381 Rz 1; Schobel, ÖBA 2004, 9

⁶⁵⁰ Avancini in Avancini/Iro/Koziol, Bankvertragsrecht I, Rz 2/137; Koziol, Haftpflichtrecht I³, Rz 3/83

⁶⁵¹ Anderst freilich wenn das offenbarte Geheimnis nicht wirtschaftlicher Natur ist sondern zur Privatsphäre zu zählen ist; Apathy/Iro/Koziol, BVR I, 315, Rz 2/154

⁶⁵² Ausführlich zu Unterlassungs-, Beseitigungs- und Schadenersatzansprüchen Apathy in Apathy/Iro/Koziol, Österreichisches Bankvertragsrecht I (2007), Rz 2/2 und Rz 2/149ff

18.1. Die Bankauskunft

Unter Bankauskünfte im engen Sinn werden die Auskünfte der Kreditinstitute über die Kreditwürdigkeit eines Geschäftspartners verstanden⁶⁵³.

Die österreichischen Privathaushalte schulden den Banken € 116,3 Mrd, die österreichischen Unternehmen € 129,5 Mrd. (siehe Kapitel 4.)

Aufgrund dieser Größenordnung ist es durchaus verständlich, dass die Kreditinstitute die Bonität sowohl der Firmenkunden als auch jener der „kleinen“ Privatkunden genau überprüfen. Zu diesem Zweck haben sie ein (fast) perfektes Informations- und Überwachungssystem installiert.⁶⁵⁴ Unter Verwendung und Abfrage von externen Datenbanken ist so ein „neuer, noch unbekannter Kunde“ bald überprüft und ziemlich „durchschaut“. Sei es, dass bei Firmenkunden neben der vorgelegten Bilanz auch noch Hintergrundinformationen über den/die Gesellschafter und Geschäftsführer, die zukünftige Entwicklung und eventuelle Negativauskünfte wie Klagen, Exekutionen abgefragt werden können, so stehen auch bei Privatkunden Datenbanken über die bisherige finanzielle Gebarung und Verpflichtungen zur Verfügung. (siehe Kapitel 10. + 11.)

Um eine Benachteiligung der Kunden entgegen zu wirken, kam es zu einer Einigung zwischen Kreditwirtschaft und Datenschutzkommission.⁶⁵⁵

Dabei wurden folgende Regelungen für die Erteilung einer Bankauskunft erstellt:

- Bankauskünfte über Geschäftskunden (juristische Personen und Selbständige) dürfen, sofern keine Weitergabebeschränkung des Kunden vorliegt, erteilt werden
- Auskünfte über Privatkunden werden nur mit deren Zustimmung erteilt (welche dadurch widerrufen werden kann)
- Betragsmäßig Angaben über Sparguthaben, Kontostände und Höhe sonstiger Verbindlichkeiten dürfen nicht erteilt werden
- Bankauskünfte erhalten nur eigene Kunden und andere Kreditinstitute, wenn ein berechtigtes Interesse glaubhaft gemacht wird

⁶⁵³ Vgl. die Nachweise bei *Apathy/Iro/Koziol*, BVR I, 326, Rz 3/2

⁶⁵⁴ Trend 11/94, 124

⁶⁵⁵ *Gola*, Betrieblicher Datenschutz, 69

Da die gesetzlichen Verschwiegenheitspflichten bei Ärzten, Rechtsanwälten, Notaren, etc. den Fällen der zulässigen Übermittlung vorgehen, umfasst dies nicht nur die mit der Geheimhaltungspflicht unterliegenden Daten beschäftigten Personen, sondern im Zweifel auch das Unternehmen selbst.⁶⁵⁶

Ein typisches Beispiel ist die Relation zwischen § 38 BWG (Bankgeheimnis) und §§ 7 und 8 DSG 2000. Kreditinstitute, ihre Gesellschafter, Organmitglieder, Beschäftigte sowie sonst für Kreditinstitute tätige Personen dürfen Geheimnisse, die ihnen ausschließlich auf Grund der Geschäftsverbindung mit Kunden oder auf Grund des § 75 Abs 3 BWG anvertraut oder zugänglich gemacht worden sind, nicht offenbaren oder verwerten.

Die Aufzählung der Bankgeschäfte in § 1 Abs 1 BWG ist nicht *taxativ*. Durch Verordnungsermächtigung iSd § 1 Abs 4 BWG kann der Bundesminister für Finanzen weitere Bankgeschäfte feststellen. Die Erteilung von Bankauskünften kann nach überwiegender Auffassung als Fall eines Bankgeschäftes angesehen werden, welches nicht im Katalog des § 1 Abs 1 BWG enthalten ist.⁶⁵⁷ Auch der Gesetzgeber sieht die Auskunftserteilung als zulässige Tätigkeit der Kreditinstitute an weil er die Erteilung „allgemein gehaltener banküblicher Auskünfte über die wirtschaftliche Lage eines Unternehmens“ als Ausnahme von der Verpflichtung zur Wahrung des Bankgeheimnisses anerkannt hat. (§ 38 Abs 2 Z 6 BWG) Gehört die Erteilung von Bankauskünften zum berechtigten Zweck von Kreditunternehmen, so ist natürlich die damit verbundene Ermittlung und Verwendung für derartige Auskünfte benötigte Daten zu bejahen, da keine schutzwürdigen Interessen des Betroffenen verletzt werden, solange nicht sein ausdrücklicher Widerspruch vorliegt.⁶⁵⁸

Banken sind den Anfragenden zur Erteilung von Auskünften besonders geeignet, da sie meist die wirtschaftlichen Verhältnisse ihrer Kunden gut kennen und aufgrund ihrer eigenen wirtschaftlichen Erfahrung diese auch meist richtig beurteilen können. Der Beantwortung solcher Auskünfte können sich die Banken idR nicht entziehen, da die Auskunftstätigkeit der Banken eine „im Kreditwesen allgemein herrschende Übung“ im In- und Ausland darstellt.⁶⁵⁹ Ohne Vereinbarung muss die Bank grundsätzlich keine Bonitätsauskünfte erteilen, selbst wenn sie von ihrem Kunden dazu aufgefordert wird; eine Pflicht zur Auskunft bedarf eines Auftrages, also der formfreien Vereinbarung (Z 7 ABB).⁶⁶⁰

⁶⁵⁶ *Krejci*, Wettbewerbsbeschränkung u. Geheimhaltungspflicht ausgeschiedener Arbeitnehmer, ÖZW 1975,1-12

⁶⁵⁷ aA *Sichtermann* der Bankauskünfte weder als Haupt- noch Nebengeschäft der Banken sieht, Das Bankgeheimnis in Deutschland, 329

⁶⁵⁸ In diesem Sinn auch *Potyka*, in *Duschanek* (Hrsg), Datenschutz in der Wirtschaft, Datenschutz im Kreditwesen, 124

⁶⁵⁹ *W. Ulrich* in *Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben, 293ff; *Schinnerer*, Bankverträge I

⁶⁶⁰ *Canaris*, BVR³, Rz 75; *Welser*, Haftung 59, OGH in ÖBA 1960,25; *Koziol* in *Iro/Koziol*, ABB Z 7, Rz 2

Der Begriff des „(Bank)-geheimnisses“ wird hier enger auszulegen sein als §§ 7 und 8 DSG 2000 da er die Arten der Verwendung von Daten im Sinne des DSG nicht umfasst. Ausnahmen dürfen nur nach den in § 38 BWG Abs 2 bis 4 angeführten Bestimmungen gemacht werden. Dies bedeutet, dass Bankauskünfte im Umfang des § 38 Abs 2 Z 6 über die wirtschaftliche Lage eines Unternehmens⁶⁶¹ abgegeben werden dürfen, was jedoch die Preisgabe konkreter Daten im Regelfall ausschließt.⁶⁶² Die wirtschaftliche Lage bestimmt sich aber nicht nur nach dem Geschäftsbetrieb sondern sind auch die privaten Vermögensverhältnisse des Unternehmers zu berücksichtigen wodurch sodann nur eine Gesamtbetrachtung ein richtiges Bild vermitteln kann.⁶⁶³ Nicht aber über andere Personen oder in anderer Form, außer bei ausdrücklicher und schriftlicher Zustimmung des betroffenen Bankkunden (§ 38 Abs 2 Z 5 BWG).

Für das Kreditunternehmen bedeutet dies bei Nichtvorliegen einer Zustimmung des Betroffenen ein Übermittlungsverbot von „Geheimnissen“, selbst wenn es für die eigenen Geschäftszwecke notwendig erscheint, oder wenn ein potentieller Empfänger überwiegend berechnete Interessen glaubhaft macht. Handelt es sich dagegen nicht um „Geheimnisse“, wohl aber um sonstige automationsunterstützte Daten, so ist ihre Übermittlung nach §§ 7 und 8 DSG zu beurteilen.⁶⁶⁴ Damit wird eine Bankauskunft über *Privatpersonen* ohne der erforderlichen ausdrücklichen schriftlichen Zustimmung (zB bei Beantragung einer bankfremden Kreditkarte) verhindert weil die Kreditunternehmung zur Wahrung des Bankgeheimnisses verpflichtet ist und dies nur mit einer ausdrücklichen schriftlichen Zustimmungserklärung des Betroffenen möglich gemacht wird.

In den Strafbestimmungen gemäß BWG und DSG 2000 kam es nun mehr zu einer Angleichung, sodass die Absicht eines Vermögensvorteils sowie der Antrag eines Verletzten vorliegen muss (§ 101 BWG und § 51 DSG 2000).

Aber auch im Falle, dass eine Bank eine Bankauskunft einem langjährigen Kunden (aufgrund eines Schuldverhältnisses) über einen Dritten erteilt, haftet sie nach stRsp⁶⁶⁵ für die erteilten Auskünfte nach § 1300 1. Satz ABGB.⁶⁶⁶ Gleich behandelt wird auch die Vertragshaftung

⁶⁶¹ Es gilt der Unternehmerbegriff iSd § 2 Abs 1 UStG 1994

⁶⁶² Feuerborn in *Sichtermann-Feuerborn-Kirchherr-Terdenge*, Bankgeheimnis und Bankauskunft³, 442

⁶⁶³ Apathy/Iro/Kozioł, BVR I, 294 ff, Rz 2/121

⁶⁶⁴ ÖZW 1979/1,17

⁶⁶⁵ OLG Innsbruck 1 R 322/89, 16.1.1990

⁶⁶⁶ § 1300 ABGB lautet: *Ein Sachverständiger ist auch dann verantwortlich, wenn er gegen Belohnung in Angelegenheiten seiner Kunst oder Wissenschaft als Versehen einen nachtheiligen Rath erteilet. Außer diesem Falle haftet ein Rathgeber nur für den Schaden, welchen er wissentlich durch Ertheilung des Rathes*

dann, wenn die Bank die Auskunft als Nebenleistung eines Vertragsverhältnisses zu erbringen hat, wobei jedoch Voraussetzung hierfür ist, dass die Auskunft noch durch das zugrunde liegende „Gesamtauftragsverhältnis“ gedeckt ist.

Vertragliche Haftungsfreizeichnungen sind nur insoweit sittenwidrig und unwirksam wenn eine grobe Fahrlässigkeit vorliegt die so schwer wiegt, dass mit einem solchen Verhalten nach den Erfahrungen des täglichen Lebens und der redlichen Verkehrsübung nicht gerechnet werden kann und sie dem Vorsatz gleichgestellt werden kann. In den heutigen AGB findet sich aufgrund der vom OGH als unwirksam angesehenen Haftungsfreizeichnungsklauseln für Verbrauchergeschäfte⁶⁶⁷ keine allgemeine Freizeichnungsklausel, auch nicht für Geschäftsbeziehungen mit Unternehmern.

Ist der Anfragende ein Unternehmer, so kann jedenfalls die Haftung für *leichte Fahrlässigkeit* ausgeschlossen werden (ABB Z9), hingegen sicherlich nicht für vorsätzliche Schädigung. Bezüglich der *grobe Fahrlässigkeit* ist die Rechtsprechung uneinheitlich und daher strittig.⁶⁶⁸ Liegt ein Verbrauchergeschäft vor, so ist nach § 6 Abs 1 Z 9 KSchG nur ein Ausschluss der Haftung für leichte Fahrlässigkeit zulässig.⁶⁶⁹ Gerade im Bereich von Bonitätsauskünften besteht der Haftungsausschluss für leichte und grobe Fahrlässigkeit zu Recht da vermieden werden soll, dass im Geschäftsverkehr das Kreditrisiko durch Einholung einer Bonitätsauskunft weitgehend auf die Bank überwälzt werden soll. Somit ist nur vorsätzliche oder krass grobe fahrlässige Schadenzufügung als sittenwidrig zu beurteilen.⁶⁷⁰

Da die ABB Z 25 von der Unverbindlichkeit der Auskunft spricht, soll hiemit die Haftung der Bank für unrichtige Auskünfte vermieden werden. Damit soll für die Bank die Verpflichtung entfallen, die Richtigkeit der Auskunft zu überprüfen.⁶⁷¹ Dadurch wird ein Haftungsausschluss erreicht, welcher im Ergebnis auch jener für grobes Verschulden entspräche.⁶⁷² Wenn es sich hierbei jedoch um die Abbedingung gesetzlicher Schutz- und Sorgfaltspflichten aus geschäftlichem Kontakt handelt, ist darin wiederum ein Haftungsausschluss zu sehen, der gegenüber Unternehmer der Inhaltskontrolle iSd § 879 Abs

dem Andern verursacht hat. Dazu Welser, Haftung der Banken für Bonitätsauskünfte, ÖBA 1982/4; Avancini – Iro - Koziol, Bankverträge I, 176, JBl 1986,168; Reischauer in Rummel, ABGB § 1300, Rz 7

⁶⁶⁷ Siehe OGH 4 Ob 179/02f, ÖBA 2003, 141 (143ff); Iro in Apathy/Iro/Koziol, BVR I, 56, Rz 1/102

⁶⁶⁸ OGH in JBl 1967, 369; EvBl 1970/312; 8 Ob 667/87 in ÖBA 1989, 89; OGH in JBl 1970, 201; vgl auch 6 Ob 541/92 in ÖBA 1993, 225 mit Anm Jabornegg

⁶⁶⁹ Wohl dann wirksam wenn kein gesondertes Entgelt für die Bankauskunft verrechnet wird; Apathy/Iro/Koziol, BVR I, 341, Rz 3/29; Koziol, HaftpflichtR, Rz 18/12 und 21

⁶⁷⁰ SZ 44/87; JBl 1977, 648; SZ 58/195

⁶⁷¹ Koziol in Iro/Koziol, ABB Z 25 Rz 3 und 4; Welser, Haftung 111ff

⁶⁷² Zur Beschränkung von Pflichten siehe Koziol, HaftpflichtR, Rz 18/30ff

3 ABGB und gegenüber Verbrauchern den Wirksamkeitsgrenzen des § 6 Abs 1 Z 9 KSchG unterläge.⁶⁷³

§ 1330 ABGB sieht sodann eine Schadenersatzpflicht vor, wenn unwahre, kreditschädigende Äußerungen verbreitet werden und davon eine Gefährdung der wirtschaftlichen Situation des beauskunftenden Unternehmens entsteht.⁶⁷⁴

Dies führte dazu, dass Kreditunternehmen Auskünfte in einem bestimmten Stil verfassen und sich die Banken auch darauf verlassen können, dass der Empfänger die Auskunft auch zu lesen versteht. Der Hinweis auf „Insolvenzgefahr“⁶⁷⁵ oder die Feststellung, dass die Bonität „noch“ oder nicht mehr zufrieden stellend sein,⁶⁷⁶ ist noch genug „allgemein gehalten“. Etwaige Bedenken müssen daher vorsichtig und möglichst Interessen schonend geäußert werden⁶⁷⁷ jedoch dürfen keine falschen oder irreführenden Angaben gemacht und für die Beurteilung der Kreditwürdigkeit wesentlichen Umstände verschwiegen werden.⁶⁷⁸

Die Auskunft darf nur feststellbare Tatsachen betreffen wie zB bestehende Liegenschaften und/oder Hypotheken, Wechselproteste, Zwangsvollstreckungen usw. Es dürfen jedoch auch Beurteilungen abgegeben werden wenn sie sorgfältig und unter Heranziehung aller Erfahrungen zum gegebenen Zeitpunkt richtig gewesen waren (auch wenn die Entwicklung nachher anders verläuft).⁶⁷⁹

Sollte die Bankauskunft von dritter Seite (von einer anderen Bank) erfolgen und die beklagte Bank nur der Vermittler dieser Auskunft sein und dies dem Kläger bekannt war, scheidet eine Gehilfenhaftung iSd § 1313a ABGB aus. Der Haftungsausschluss wird nämlich bereits schon dann schlagend, wenn die Bank zu erkennen gibt, dass sie über keine besondere Sachkunde über diese Auskunft verfügt und mitteilt, was sie selbst von dritter Seite erfahren hat. In einem solchen Fall käme bloß die Haftung nach § 1300 Satz 2 ABGB in Betracht wenn die Kenntnis der Unrichtigkeit der Auskunft angenommen werden kann.⁶⁸⁰

Bei der deliktischen Haftung ist keine Schädigungsabsicht erforderlich, sondern reicht schon Schädigungsfahrlässigkeit aus.⁶⁸¹ Rat und Auskunft werden von der hA iSd § 1300 Satz 2

⁶⁷³ Koziol, BVR I, Rz 3/19 und 20

⁶⁷⁴ JBl 1986, 168 ff [Welser, 119]; WBl 1989, 350; Pawlikowsky, Datenschutz: Leitfaden & Materialien, 144

⁶⁷⁵ Avancini, BVR I, Rz 2/113

⁶⁷⁶ Jabornegg, ÖBA 1997, 673

⁶⁷⁷ OGH in JBl 1981, 425 und (nicht veröffentlicht) 4.4.1984, 3 Ob 600/83; Jabornegg, ÖBA 1997, 673

⁶⁷⁸ Jabornegg, ÖBA 1997, 673; Apathy/Iro/Koziol, BVR I, 296, Rz 2/123

⁶⁷⁹ Scheerer, Probleme der Haftung der Kreditinstitute für die Erteilung von Auskünften in D und F unter besonderer Berücksichtigung der Haftungsfreizeichnungsklauseln, Bärmann-FS (1975), 803

⁶⁸⁰ Koziol, Haftpflichtrecht II 188; Avancini – Iro – Koziol, Bankverträge I, 177

⁶⁸¹ So Koziol in Apathy/Iro/Koziol, BVR I, 329, Rz 3/8; anders jedoch OGH, zB 4 Ob 252/00p in ÖBA 2001, 819

ABGB gleichgestellt da es aufgrund einer Irreführung zur Herbeiführung eines reinen Vermögensschadens geht.⁶⁸²

Da eine Bankauskunft prinzipiell das Recht auf informelle Selbstbestimmung verletzt, müsste der Kunde darüber informiert werden, wer sich für seine wirtschaftliche Situation interessiert und welche Informationen weitergegeben wurden.

Der OGH⁶⁸³ betont in nunmehr stRsp, dass die Bank zukünftige Bürgen bzw Diskontnehmer auch ohne dessen ausdrückliche Anfrage über die drohende oder bestehende Insolvenz des Kreditnehmers bzw Akzeptanten in geeigneter Weise aufzuklären hätte, wobei die durch die Bank in solchen Fällen abzugebenden Erklärungen idR über eine allgemein gehaltene, bankübliche Bankauskunft hinausgehen.⁶⁸⁴

⁶⁸² OGH in JBl 1979, 88; JBl 1981, 319; 8 Ob 667/87 in ÖBA 1989, 89; *Reischauer* in *Rummel*, ABGB², § 1300 Rz 1; *Welse*, r Haftung 11ff mwN; *Ehrenzweig* II/1, 665,

⁶⁸³ OGH 9.2.1988 6 Ob 508, 509/86 = RdW 1988, 130; OGH 7.9.1988, 8 Ob 629/89 = ecolex 1990, 18; EvBl 1983/128; 1984/160

⁶⁸⁴ *Laurer*, Das Bankgeheimnis in der Entwicklung von Lehre und Rechtssprechung, ÖJZ 1986, 385ff; *Weissel*, Die Negativliste der Banken aus datenschutzrechtlicher Sicht, EDVuR 1990, 62

19. Das Zentrale Melderegister (ZMR)

Gemäß § 16a Abs. 5 MeldeG war eine beschränkte Abfrage des Zentralen Melderegisters durch Personen AUSSERHALB der öffentlichen Verwaltung („sonstige Abfrageberechtigte“ gem. § 1 Z 4 MeldeV) zulässig, die einen regelmäßigen, rechtlich begründeten Bedarf nach Meldeauskünften bescheinigen können, wie z.B. Notare, Rechtsanwälte, Banken, Versicherungen, Mobilfunkbetreiber, etc.

Privatpersonen können auch – gegen Entgelt – ihre Daten sperren lassen. Dies nützt jedoch nichts, wenn Behörden oder Rechtsanwälte, Notare diesbezüglich Anfragen stellen.

Aufgrund zahlreicher Artikel erregte die vertrags- und gesetzwidrige Verwendung von Meldedaten durch Abfrageberechtigte erhebliches Aufsehen in der Öffentlichkeit. Auch die etwas „unglückliche“ Bezeichnung der Abfrageberechtigten als „Business-Partner“ in der einschlägigen Verordnung des BMI⁶⁸⁵ förderte das Misstrauen und die Aufregung weil dadurch (auch wenn überhaupt nicht beabsichtigt) der Eindruck erweckt wurde, Meldedaten seien „Handelsware“ und würden gegen Geld weiterverkauft. Es kam danach zum Entzug von einigen Berechtigungen wobei jedoch in zumindest einem Fall die Maßnahme erfolgreich beim VwGh bekämpft wurde.⁶⁸⁶

Gemäß § 30 Abs 2 DSG 2000 kann die Datenschutzkommission im Falle eines begründeten Verdachtes auf Verletzung der Rechte oder Pflichten eines Auftraggebers oder Dienstleisters Datenanwendungen überprüfen. Dies hat die Datenschutzkommission zur Einleitung eines Prüfverfahrens im Jahr 2003 bewogen. Durch eine Vorort Überprüfung konnten anhand diverser Suchlogarithmen Ergebnisse erzielt werden welche so nie vorgesehen waren und welche einen möglichen Missbrauch zu fördern schienen. („wild card“ Suche, Auswahl aus Trefferliste, etc.)

Eine Verwendung von ZMR-Daten durch sonstige Abfrageberechtigte für Zwecke Dritter ist vom Gesetz untersagt. Ein sonstiger Abfrageberechtigter darf in keiner Form, auch nicht durch Ermöglichung einer indirekten Abfrage, per Briefpost, Fax, E-Mail oder per Telefon, ZMR-Daten an Dritte übermitteln. Jede einzelne Abfrage des ZMR muss nachweislich dem Zweck der eigenen 'erwerbsmäßigen Geltendmachung oder Durchsetzung von Rechten oder Ansprüchen' dienen. Dies umfasst freilich auch die berufsmäßige Parteienvertretung durch Rechtsanwälte, Notare und vergleichbare Tätigkeiten, die ihnen übermittelte ZMR- Daten

⁶⁸⁵ VO über die Bestimmung der Support-Unit Zentrales Melderegister (ZMR) als Organisationseinheit, bei der die Flexibilisierungsklausel zur Anwendung gelangt, BGBl. II Nr. 20/2003

⁶⁸⁶ DSB 2005, 33ff, VwGh vom 16.12.2003, 2003/05/0078

dazu verwenden, um namens und im Auftrag eines Mandanten dessen Rechte und Ansprüche durchzusetzen, was zumindest im Wortsinn von § 16a Abs 5 MeldeG noch Deckung findet und erkennbar von Ziel und Zweck des Gesetzes umfasst ist.

Auch der berufsmäßige Parteienvertreter darf aber ZMR-Daten nur im Zusammenhang mit der Durchsetzung von Rechten und Ansprüchen, also etwa zwecks Adressierung einer Klage oder Namhaftmachung eines Zeugen, verwenden. Einen bloßen Auftrag zur Ermittlung von Meldedaten für einen Mandanten durch ZMR-Abfrage darf er nicht übernehmen.

Die DSK sah sich nach Durchführung des Kontrollverfahrens zu einer Empfehlung gemäß § 30 Abs 6 DSG 2000 an das BMI gezwungen wobei aufgetragen wurde, dass durch programmtechnische Maßnahmen sichergestellt werden soll, dass Abfrageergebnisse nicht gegen Entgelt an Dritte übermittelt werden.⁶⁸⁷

Gesamtsumme aller aktiven Personen im ZMR (Stichtag 1.1.2008):⁶⁸⁸ 9,446.853

Anzahl eindeutiger Treffer mittels Familienname + Vorname(n) + Geburtsdatum: 9,303.641

Anzahl mehrdeutiger Treffer mittels Familienname + Vorname(n) + Geburtsdatum: 143.212 (dahinter verbergen sich 71.194 "Personendoppel" mit gleichen Namen und Geburtsdatum, der Maximalwert einer Suche ergab 4 Personen)

Anzahl eindeutiger Treffer mittels Familienname + Vorname(n): 5,334.754

Anzahl mehrdeutiger Treffer mittels Familienname + Vorname(n): 4,112.099 (dahinter verbergen sich 974.946 "Personendoppel" mit gleichen Namen, der Maximalwert einer Suche ergab 800 Personen)

Anzahl eindeutiger Treffer mittels Familienname + Geburtsdatum: 8,592.526

Anzahl mehrdeutiger Treffer mittels Familienname + Geburtsdatum: 854.327 (dahinter verbergen sich 399.734 "Personendoppel" mit gleichen Familiennamen und Geburtsdatum, der Maximalwert einer Suche ergab 17 Personen)

Die steigende Bedeutung des ZMR lässt sich auch aufgrund der ständig steigenden Zahlen und Einnahmen ermessen.⁶⁸⁹

⁶⁸⁷ Der ganze ausführliche Text ist unter GZ K213.002/008-DSK/2003 vom 9. Mai 2003 im Internet abrufbar

⁶⁸⁸ Quelle: BMI, Abt. SU-ZMR

⁶⁸⁹ Quelle: BMF, Abt. II/7; genauere Daten für 2006, 2007 und 2008 wurden trotz mehrfacher Urgenz weder von Seiten des BMF noch des BMI bekannt gegeben

Jahr	Anzahl der Abfragen	Einnahmen des BMI
2003	878.434	€ 2,227 Mio
2004	971.622	€ 2,333 Mio
2005	1.263.149	€ 2,763 Mio
2006	1.200.000 (geschätzt)	€ 2.715 Mio
2007	1.400.000 (geschätzt)	€ 3,041 Mio
2008	---	€ 3,000 Mio (budgetiert)

20. Schlussbemerkungen

Information(en) sind heutzutage ein wichtiger Rohstoff für das Wirtschaftsleben so wie es Erdöl für die Industrie ist. Sie sind eine nie versiegende Quelle. Es gilt sie nur richtig und rechtmäßig zu nutzen und dabei niemanden zu übervorteilen bzw. zu benachteiligen und je mehr sie be- und genutzt werden desto ergiebiger ist auch der Ertrag wenn die „Spielregeln“ eingehalten werden. *Castells*⁶⁹⁰ nennt es prägnant „erstmal verwenden wir Information und Kommunikation, um primär wieder Information und Kommunikation zu erzeugen und zu verarbeiten...Information wird selbst zum primären Gut“. Die Computer und in weiterer Folge das Internet geben uns fast unerschöpfliche Informationsquellen in vernachlässigbarer Zeitverzögerung zur Wirklichkeit und speichern Informationen von gestern für heute, morgen und übermorgen.

Durch das bestehende DSG 2000 kam es zum Wegfall der Zweigleisigkeit der Regelungen für den öffentlichen und privaten Bereich und durch Standard- und Musteranwendungen zur wesentlichen Reduzierung der Registrierungspflichten beim DVR. Auch die Zuständigkeit der DSK für Verletzung von Auskunftspflichten ermöglicht nun eine schnellere und effizientere Durchsetzung der Rechte des Betroffenen. Andererseits gibt es noch immer sehr viele unbestimmte Rechtsbegriffe zB im Bereich der Informationspflicht oder des Widerspruchrechts wodurch Auftraggeber einen komplexen Sachverhalt im Einzelfall beurteilen müssen und es dadurch oft zu Missverständnissen oder vermeintlichen Datenschutzverletzungen kommt die jedoch in dieser Art und Weise nicht beabsichtigt sind weil aufgrund der Komplexität des Datenschutzgesetzes viele Auftraggeber einfach damit überfordert sind und auch nicht immer ausgebildete Juristen zur Verfügung stehen.

Beim Studium von vielen Entscheidungen der DSK, des VwGH und des VfGH kam ich zur Erkenntnis, dass ca. 40 – 50 % der geführten Verfahren de facto eigentlich unnötig gewesen wären wenn der Betroffene die richtigen und vollständigen Auskünfte zur richtigen Zeit erhalten hätte und diese nicht zuerst einmal gar nicht und dann erst „zizerlweise“⁶⁹¹ herausgerückt wurden oder es auch ganz einfach am Verständnis und Wissen des DSG auf beiden Seiten mangelte.

Eine Überlegung wäre daher die angedachten, vom Gesetz geforderten Datenschutzbeauftragten von Unternehmen in Österreich zu regelmäßig stattfindenden

⁶⁹⁰ *Castells*, The rise of the Network Society, 32ff, 66ff, 154ff

⁶⁹¹ = kleinen Stücken. Laut Wehle möglicherweise von "Zizerl" = "Zaunkönig", ein besonders kleiner Vogel;
www.janko.at

Informations- und Schulungsveranstaltungen zu schicken und auch gleichzeitig die Rechte und Pflichte dieser im DSG 2000 zu verankern und dadurch sowohl den Auftraggebern als auch den Betroffenen zu ihren Rechten (und auch Pflichten) rasch, unkompliziert und umfassend zu verhelfen. (was durch die Einführung des § 15a in der DSG Novelle 2008 bereits geplant ist)

Für Betroffene besteht im privaten Bereich (abgesehen vom Auskunftsrecht) noch immer das Prozessrisiko durch Einbringung einer Klage beim zuständigen Landesgericht. Dies wurde aus dem Gedanken auf die Notwendigkeit der Bündelung der Verfahren seinerzeit festgelegt.⁶⁹² (§ 29 Abs 1 DSG 2000). Die Praxis zeigt jedoch, dass sich bis dato keine einheitliche und logisch nachvollziehbare Sach- und Entscheidungskompetenz entwickeln konnte und die Devise „näher zum Bürger“, eventuell auch eine Zuständigkeit des Bezirksgerichtes überlegenswert macht. Auch eine damit verbundene (niedrige) Deckelung des Streitwertes würde eine einfachere Rechtsdurchsetzung für den Betroffenen ermöglichen. Nachdem der Bereich Datenschutz trotz seines relativ geringen Gesetzesumfanges eine komplizierte und äußerst weitschichtige Materie ist, würde ich nicht von der Verpflichtung der anwaltlichen Vertretungspflicht abgehen obwohl (Rechts-)Experten auf diesem Gebiet auch sehr dünn gesät sind. Das Datenschutzrecht mit dem fast jeder täglich irgendwie konfrontiert wird (auch wenn er es bewusst gar nicht weiß), hat sich zur hochkomplexen Materie entwickelt. Jedoch nur die Schuld beim österreichischen Gesetzgeber zu suchen, trifft nicht exakt den Kern der Sache weil schon die komplexen Vorgaben aufgrund der Datenschutz RL 95/46/EG verursacht wurden und es aufgrund der bereits genannten Kompetenzregelungen zwischen Bund und Länder zu einer weiteren (gedanklichen) Zersplitterung kommen musste. Aber wie der Name schon sagt, handelt es sich um eine Richtlinie welche mit einem gewissen Entscheidungsspielraum vom nationalen Gesetzgeber umzusetzen ist. Der VfGH hat in seinem berühmten „Denksporterkenntnis“⁶⁹³ bereits ausgeführt, dass *„eine Norm dann den Boden des rechtsstaatlichen Prinzips verlässt, wenn sie nur mit subtiler Sachkenntnis, außerordentlichen methodischen Fähigkeiten unter einer gewissen Lust zum Lösen von Denksportaufgaben verstanden werden kann.“*

Obwohl die Anfragen und Beschwerden bei der DSK seit Jahren im Steigen begriffen sind, besteht prinzipiell noch immer eine geringe Bereitschaft der Bevölkerung, ihre Datenschutzrechte auch aktiv einzufordern. Unternehmen tun daher gut daran interne Richtlinien zur Auskunftsbearbeitung/-erteilung zu erstellen worin festgelegt wird welche

⁶⁹² Dohr-Pollirer-Weiss, Anm 3 zu § 39, DSG, 120

⁶⁹³ VfGH 7.12.1989, 12.240

Daten der Auskunftspflicht unterliegen und wo keine Pflicht zur Auskunftserteilung besteht. Denn nur wer seine Rechte kennt, weiß sie auch einzusetzen. Wie auch viele Entscheidungen der DSK zeigen, ist vielen belangten Auftraggebern der unerlaubte Eingriff in das verfassungsrechtlich geschützte Recht auf Datenschutz überhaupt nicht bewusst, vielmehr glaubten sie sogar ein Recht zur Datenverwendung zu haben.⁶⁹⁴ Der Bürger muss wach gerüttelt werden, er muss Problembewusstsein entwickeln ! Hier ist vor allem die Politik gefordert den erheblichen Informations- und Schulungsaufwand für den Einzelnen zu befriedigen, ihn über seine Rechte (und auch Pflichten) aufzuklären und damit Unklarheiten, Un- und Halbwahrheiten Einhalt zu gebieten.⁶⁹⁵

Durch das Urteil des OGH vom 2.10.2003 6 Ob 192/03h (siehe Kapitel 3.4.) wurde ja eine Erkundigungspflicht für Gläubiger bei Verdacht der Zahlungsunfähigkeit statuiert. Da es sich hierbei um eine bestehende Geschäftsbeziehung handelt wo sich Gläubiger und Schuldner schon über einen längeren Zeitraum „kennen“, ist es doch eigentlich aufgrund eines Umkehrschlusses erst recht notwendig, neue Geschäftsbeziehungen bzw. in Anbahnung befindliche, einer genauen Prüfung zu unterziehen. Es wird ja auch niemand von einer Bank verlangen können, dass sie Kredite ohne vorherige Prüfung der finanziellen Situation des Kreditnehmers vergibt. Es ist daher auch der sonstigen „kreditgewährenden Wirtschaft“ wie zB Versandhäuser, Mobilfunkunternehmen, Versicherungen, etc. das Recht, Erkundigungen in Bezug auf ihre Zahlungsfähigkeit über ihre sowohl bestehenden als auch neuen Kundenbeziehungen zu zugestehen.

Durch das rechtskräftige Urteil des OGH Wien bezüglich des Widerspruchsrecht von Bonitätsdaten (siehe Kapitel 14.3.1.) wird jedoch die Sinnhaftigkeit und Aussagekraft von Bonitätsauskünften generell in Frage gestellt. Auch wenn das Urteil rein formal rechtlich einwandfrei ist und das Sozialministerium jubelt, muss man sich allen Ernstes fragen, wem nützt diese Regelung und wer wird sie (aus-)nutzen und negative Auskünfte löschen lassen wollen ? Kann es der Telos des Gesetzes sein sich so unerwünschter Daten (auch wenn sie richtig sind) mit einem Streich zu entledigen ? Natürlich in den meisten Fällen nur jene, die damit ein weiterführendes Ziel bezwecken um wieder in den Genuss von finanziellen Mitteln zu kommen die sie sonst auf „normalen“ Wege garantiert nicht erhalten würden. Sowohl das

⁶⁹⁴ zB K120.986/0013-DSK/2005 vom 20. Mai 2005

⁶⁹⁵ In einer Befragung [Sample 1213 d. österreichischen Wohnbevölkerung ab 16 Jahre) sagen 77 %, dass sie mehr oder weniger ahnungslos in Bezug auf Datenschutzbestimmungen sind. 92 % wissen nicht ob bzw. wer Daten über sie sammelt und 76 % sagen, dass die Bevölkerung nicht ausreichend über Datenschutz, Missbrauch- Risiken und rechtliche Gegebenheiten informiert ist. (siehe dazu www.austria.gv.at/site/3462/default.aspx), Der Standard, 16.7.2008, 14

OLG als auch der OGH erkennt die Tatsache, dass es ja (in diesem Fall der zukünftige) Mobilfunkkunde ist, der dem Mobilfunkbetreiber ein Angebot stellt und dieser es annehmen oder ablehnen kann. Ein Kontrahierungszwang aufgrund der Vielzahl der Betreiber erscheint ausgeschlossen. (nebenbei handelt es sich bei einem Mobilfunkvertrag sicherlich nicht um ein wesentliches Element der Daseinsversorgung wie Strom, Gas, Wasser, Heizung). Die AGB's des Mobilfunkbetreiber kommen sicherlich erst bei Annahme des Angebots dh bei Freischaltung der SIM Karte in Geltung aber eine am Antrags-/Angebotsformular gemachter Hinweis auf eine allfällige Bonitätsprüfung VOR Freischaltung kann in Kenntnis dieser Sachlage in diesem Fall als gültige Willenserklärung iSd § 4 Z 14 DSG 2000 angesehen werden und mindert sicherlich nicht deren Gültigkeit.

Alle Auskunfteien und Kreditschutzverbände hofften auf ein korrigierendes und abschließendes Urteil zum § 28 Abs 2 DSG 2000 durch den OGH welcher sich nicht nur nach den Buchstaben des Gesetzes richtet sondern auch den Sinn und die Zweckmäßigkeit dieser Regelung ein für alle mal festlegt. Leider wurden damit alle diesbezüglichen Datenverarbeiter (Auftraggeber und Dienstleister) enttäuscht.

Nachdem dieses Urteil in der Öffentlichkeit sicherlich für großes Echo sorgen wird, werden sämtliche Kreditinformationsanbieter in den nächsten Monaten und Jahren tausende von Anträgen erhalten wo Kunden ihre in der Vergangenheit verursachten Negativeinträge wie Exekutionen, abgelegte Vermögensverzeichnisse, etc. „tilgen“ wollen um wieder von „vorne“ beginnen zu können. Dies vielleicht auch gerade dann wenn die Schuld bei vorigen Vertragspartner noch nicht einmal vollständig zurückbezahlt wurde.

Ist sich jemand überhaupt der Folgen bewusst wenn es aufgrund eines nicht ordnungsgemäß erfüllten Vertrages zu einem neuerlichen Negativeintrag kommt ? Der Kunde lässt den Negativeintrag wieder löschen gem. § 28 DSG 2000 und geht zum nächsten Kreditinstitut/Mobilfunkanbieter/Versandhandelunternehmen usw. und beginnt wieder von vorne solange bis alle jeweiligen potentiellen Vertragspartner „abgeklappert“ wurden und der Name dort aufgrund der zu betreibenden Maßnahmen als „unerwünscht“ aufscheint ? Intelligente, professionelle Schuldner werden dies auf Jahre hinaus spielen können und dabei offene Beträge verursachen die dann wohl in höheren Zinsen, Tarifen, Gebühren, komplizierteren Geschäftsbedingungen (zB nur mit Bürgen, nur gegen Vorauszahlung, etc.) für die Allgemeinheit Niederschlag finden werden.

Es stellt sich daher die Frage was nun schwerer wiege: der Datenschutz des Einzelnen, oder der Gläubigerschutz und in weiterer Folge der Schutz der Wirtschaft und gesamten Volkswirtschaft und auch die Möglichkeit der weiteren Verschuldung von Privaten und Firmen Einhalt zu gebieten.

Diese Entscheidung ist daher aus (volks-)wirtschaftlichen und praktischen Gründen strikt abzulehnen.

Für alle negativen Dateneinträge besteht einerseits eine gesetzliche Lösungsverpflichtung gemäß § 27 DSG 2000 wenn die Daten unrichtig oder nicht mehr aktuell sind andererseits auch eine von der DSK vorgegebene Löschungsvorgabe in den marktbeherrschenden Kreditinformationsdatenbanken. Natürlich wäre eine diesbezügliche genaue, für alle verbindliche, gesetzliche Regelung für eine Verwendung und Lösungsverpflichtung äußerst zu begrüßen um hier schon im vorhinein vielen administrativen Schreibaufwand und Unklarheiten auf beiden Seiten zu beseitigen. Bis dato fehlt leider noch immer eine Regelung wann ein Inkassobüro welche Daten an wen weitergeben darf.

Da die Aktualität und Richtigkeit von Daten immer von ihrer Herkunft bestimmt wird, sollte auch äußerst Bedacht genommen werden, dass die Nachvollziehbarkeit gewahrt bleibt und es im negativen Fall besser wäre, diese umgehend zu löschen. Hier sind natürlich die Datenverarbeiter von ihren Datenbezugsquellen abhängig. Eine Lösung sehe ich hier in der verpflichtenden Übermittlung einer Geschäfts- oder Aktenzahl um etwaige Negativeinträge schnell und unbürokratisch verifizieren zu können.

Weiters ist die bereits im Bereich der Adressverlage und Direktmarketing Unternehmen erfolgreich praktizierte Selbstkontrolle („Code of conduct“ oder auch „binding corporate rules“)⁶⁹⁶ auch für Kredit- und Wirtschaftsauskunfteien eine intensivere Überlegung wert. Selbstregulierungsbereiche ergeben sich oft dann, wo eine Menge an Beschwerden in Verbindung mit einer komplizierten Materie auftritt. Ein damit verbundenes „Gütesiegel“⁶⁹⁷ würde die erfolgreichen und etablierten Unternehmen auszeichnen und auch als eine Art Wettbewerbsvorteil gesehen werden können und dadurch eine positive publicity für die jeweiligen Unternehmen und den Großteil der Branche schaffen. Allerdings ist auch anzumerken, dass die Verhaltensregeln des Art 27 DS-RL aufgrund der fehlenden Bindungswirkung gegenüber Dritten und der fehlenden gerichtlichen Durchsetzbarkeit eher zu einem „stumpfen Schwert“ mutieren und es jedem Mitgliedsstaat unbenommen bleibt, eigene nationale gesetzliche Rechtsvorschriften zu erlassen.⁶⁹⁸ Eine Förderung des „aktiven Datenschutzes“ wie es etwa in Deutschland praktiziert wird,⁶⁹⁹ durch standardisierte

⁶⁹⁶ Die ersten „Codes of conduct“ wurden in Deutschland für Daimler Chrysler von *Büllesbach* entwickelt. Siehe dazu *Büllesbach-Dreier* (Hrsg), Konvergenz in Medien und Recht (2002), Konvergenz durch Standardisierung und Selbstregulierung

⁶⁹⁷ *Brühann*, DuD 1996, 66 (69), bezeichnet eine Unbedenklichkeitsbescheinigung nach Art 27 Abs 3 DS-RL als eine Art „Gütesiegel“. Dies kommt der Zertifizierung aufgrund eines Audit Verfahrens schon recht nahe obwohl die RL in Art 27 nicht von einer gesetzlichen Schaffung eines Audit Verfahrens spricht.

⁶⁹⁸ *Ehmann/Helfrich*, EG DS-RL, Art 27 Rn 9

⁶⁹⁹ § 9a BDSG Datenschutzaudit lautet: *Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr*

Vorgaben und Verfahren, hätte sicherlich einen positiven Einfluss auf die gewünschte Selbstregulierung dieser Branche.

Dies hätte auch die positiven „Nebeneffekte“, dass sich die jeweiligen Unternehmen in der „Auskunfteibranche“ intensiv mit dem Thema Datenschutz auseinandersetzen müssten und neben der Einheitlichkeit auch ein Lerneffekt in Bezug auf datenschutzrechtliche Regelungen vorhanden wäre. Die Endkontrolle müsste natürlich den staatlichen Stellen vorbehalten sein um die Einhaltung des DSG als Mindeststandard zu garantieren.

Es würden sich hiezu zwei Ansätze ergeben: Entweder werden durch eine staatliche Behörde Verträge abgeschlossen oder die Wirtschaftsauskunfteien loben einseitig gegenüber Dritten die Einhaltung dieser Verhaltensregeln aus wobei die Betroffenen Drittbegünstigte sein sollten.

Die „regulierte Selbstregulierung“⁷⁰⁰ hätte auch durchaus Chancen auf Verwirklichung in Österreich wenn das bereits erwähnte Wissen über Datenschutz verstärkt und auch mit Hilfe des Staates gefördert wird und es zu keinem Ungleichgewicht der Kräfte bzw. der Marktteilnehmer kommt.

Pleiten von Privaten und Firmen werden nie zu verhindern sein. Genauso wenig private Katastrophen und ihre finanzielle Folgen die daraus resultieren. Die EU sollte zu einer Verbraucherkreditlinie finden, die Kreditkonditionen Transparenz verordnet und eine Gesamtprüfung der Bonität von Privatkunden und viel umfassendere Informationen und Warnungen vorschreibt.

Denkbar wäre die Einrichtung eines verpflichtenden zentralen Kleinkreditkatasters. Einblick und Zugriff hätte lediglich der Schuldner. Will er einen Kredit aufnehmen oder ein Kredit-/Zielgeschäft abschließen, so druckt er sich dieses Katasterblatt aus und legt dieses beim beabsichtigten Geschäftsabschluss vor.⁷⁰¹ Dadurch würde auch die in der Allgemeinheit kursierende „Geheimnistuerei“ und das „gefährliche Halbwissen“ ein Ende finden und mehr Transparenz würde in den Markt der Kreditauskünfte/Bonitätsbeurteilungen einkehren.

Als Folge von Basel II welches eine neue Art der Risikobewertung und damit klare Richtlinien für die Eigenkapitalunterlegungspflicht der Banken vorschreibt, werden auch immer mehr „Positivdaten“ von Kreditnehmern wichtig. Darin wird der Kunde als Ganzes

Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

⁷⁰⁰ So bezeichnet von Knyrim in 25 Jahre Datenschutzrecht in Österreich, MR 2005, 415

⁷⁰¹ Der Standard, 8.6.2004

einer Überprüfung unterzogen. So auch auf seine gesamte Vermögenslage, den Lebensstil, Gesundheitszustand, Managementqualitäten bis zu den jeweiligen familiären Verhältnissen. Die Eingriffstiefe in diese dann doch sehr persönlichen Bereiche erfordert, sofern überhaupt eine diesbezüglich Notwendigkeit besteht, ein Höchstmaß an Sensibilität bzw. sogar eine eigene rechtliche Normierung.

Aber sollten auch die Strafbestimmungen des § 282ff UGB deutlich erhöht bzw. verschärft werden um den Gläubigerschutz vor eigenen wirtschaftlichen Interessen zu stellen. So beträgt zB bei großen Kapitalgesellschaften die Zwangsstrafe maximal das Sechsfache des Grundbetrages von € 3.600,-- somit maximal € 21.600,-- (zusätzlich zu den zuvor verhängten Zwangsstrafen insgesamt maximal € 28.800,--) Dieser Betrag ist für Unternehmen welche hunderte Euro Millionen jährlich umsetzen nicht viel mehr als ein kleiner Griff in die „Portokasse“. Zu denken wäre hier nicht nur an eine massive Erhöhung dieser Beträge sondern auch an eventuelle Beuge(haft-)strafen gegenüber den geschäftsführenden Organen jedoch müsste dies EU weit für alle Staaten gelten um eine „Gleichheit der Waffen“ zu gewährleisten.

Sehr interessant erscheinen mir die Vorarbeiten und Überlegungen für die Schaffung eines datenbankgestützten Mobiliarpfandregisters welches ähnliche Zugriffsmöglichkeiten gewähren soll wie das Firmenbuch (Einsicht „auf Verlangen“ § 33 FBG). Natürlich müssen hier auch datenschutzrechtliche Barrieren eingebaut werden um „Neugierige“ von einem undifferenzierten „Blättern“ aus Lust und Laune abzuhalten aber andererseits dem berechtigtem Interesse Dritter und dem Schutzbedürfnis des betroffenen Pfandgebers gerecht zu werden. Die prinzipielle Führung dieses Registers sollte aber einer öffentlichen Stelle wie zB beim Firmenbuch oder Grundbuch, vorbehalten bleiben um die Frage der Publizitätswirkung eindeutig regeln zu können. (sofern dies beabsichtigt ist). Natürlich ist diese Datenbank wiederum ein weiterer Mosaikstein um Teilnehmer am Wirtschaftsleben besser kennen zu lernen und zu überprüfen – Kritiker würden sagen „zu durchleuchten“ – aber andererseits ist Gefahr des exzessiven Missbrauchs (siehe Grundbuch) eher als gering einzuschätzen und als wirtschaftliche Datenbank in dieser Hinsicht voll zu begrüßen.

Auch in Bezug der Aufgabentrennung der staatlichen Datenschutzeinrichtungen besteht ein Verbesserungs- und Anpassungsbedarf. Die DSK ist einerseits Entscheidungsinstanz für den öffentlichen Bereich, andererseits kann sie im privaten Bereich als Gutachterin in Zivilprozessen (§ 29 Abs 3 DSG 2000) auftreten oder muss sogar bei Verlangen eines

Betroffenen und bei Vorliegen der Voraussetzungen des § 29 Abs 4 DSG 2000 als Neben-intervenient beitreten. (siehe Kapitel 16.) Im öffentlichen Bereich erfüllt die DSK einerseits die Rolle einer Aufsichtsbehörde andererseits muss sie bei Individualbeschwerden als unabhängige Instanz entscheiden.

Die laufenden datenschutzrechtlichen Agenden und zur Unterstützung der Geschäftsführung in der DSK nimmt die im Verfassungsdienst des Bundeskanzleramt (BKA) eingerichtete Geschäftsstelle wahr⁷⁰².

Seit Mitte 2006 besitzt die Geschäftsstelle zwei Referate – das Büro der DSK, das für die vorbereitende Behandlung der Beschwerdefälle zuständig ist, und das Datenverarbeitungsregister (DVR). Auch hier ist wieder die Politik gefordert um die Verflechtung der in Personalunion im Büro des BKA angesiedelten Personen als auch in der DSK die mit der ausgestatteten Entscheidungskompetenz für den öffentlichen Bereich, zu entflechten. Handelnde Personen im Büro des BKA sind einerseits Advokaten des Datenschutzes (zB bei der Vorbereitung von Stellungnahmen des Datenschutzrates zu geplanten Gesetzen) als auch in Entscheidungen der DSK eingebunden. Dass dies aus verständlichen Gründen zu einer problematischen Konstellation führt, braucht nicht weiter erläutert werden. Aufgrund des über Jahre gesammelten Wissens im Datenschutzbüro des BKA steht auch der Vorschlag eines „Bundesdatenbeauftragten“ als komplett unabhängiges und weisungsfreies Organ zur Diskussion welcher sich bei Stellungnahmen zu Gesetzesentwürfen nicht mehr zurück halten bräuchte weil er in weiterer Folge (nicht mehr) auch Entscheidungsinstanz wäre.⁷⁰³ Am System der dualen Rechtsdurchsetzung bei Gericht und bei Verwaltungsbehörden ändert dies nichts weil Streitigkeiten zwischen Betroffenen und für die Verarbeitung Verantwortlichen nun mal zivile Streitigkeiten darstellen, für die in Österreich das Streitbeilegungsinstrument der Zivilgerichtsbarkeit geschaffen wurde und sich auch schon jahrzehntelang erfolgreich bewährt hat. Jedes Grundrecht ist natürlich nur soviel wert, sofern auch die Möglichkeit besteht, dieses durchzusetzen. Bedauerlicherweise ist in diesem Zusammenhang auf die Einleitung eines Vertragsverletzungsverfahrens vor der Europäischen Kommission zu verweisen um die Unabhängigkeit der Datenschutzkommission herzustellen, damit diese endlich wirklich unabhängig wird und zwar in Form von eigener Personal- und Budgethoheit.

⁷⁰² § 35 Abs 2 DSG 2000; zur Praxis vgl DSB 1993, 25 der von einem „gemeinsam für den Datenschutzrat (DSR) und die DSK im organisatorischen Rahmen BKA-Verfassungsdienst (Abteilung V/3) eingerichteten Geschäftsapparat (Datenschutzbüro)“ spricht

⁷⁰³ *Mayer-Schönberger-Zeger-Kronegger*, Auf dem Weg nach Europa, Zur Novellierung des DSG, ÖJZ 1998, 249

In einem Gesetzesentwurf (BKA-603.363/0018-V/A/1/2007; 94/ME XXIII.GP) zur Verwaltungsreform soll die DSK abgeschafft werden und deren Kompetenzen auf neun Verwaltungsgerichtshöfe aufgeteilt werden. Diese „Reform“, möge sie auch ehrenhafte Ziele im Sinn haben, geht meines Erachtens fast vollständig am Bürger vorbei und schafft nur eine weitere Zersplitterung und Chaos bei den Zuständigkeiten weil die Gerichtshöfe erst ihre örtliche und sachliche (Un-)Zuständigkeit erklären müssen und der Bürger mit seinem Anliegen im „Kreis geschickt“ wird.

Bei einem Blick über die Landesgrenzen, zu unserem deutschen Nachbarn erkennt man, dass es dort 16 unabhängige, mit eigenem Budget ausgestattete Landesdatenschutzbehörden und eine Bundesstelle gibt.⁷⁰⁴

Als äußerst bedenklich erachte ich die Abschaffung des Grundrechts auf Datenschutz für juristische Personen in der DSG Novelle 2008. (BKA-810.026/0002-V/3/2008). Das derzeitige Verhältnis von Offenlegungs- und Geheimhaltungspflichten bei juristischen Personen sehe ich als ausreichend an. Es gibt keinen spezifischen Grund das Datenschutzniveau in diesem Bereich auf das niedrigere Niveau in anderen europäischen Ländern anzupassen welches sodann zu Problemen im Bereich des Rechtsschutzes bei Geschäfts- und Betriebsgeheimnisse führen kann.

Ein zutreffender Vergleich fasst die Durchsetzung von Rechtsregeln in diesem Bereich wie folgt zusammen: *Wer allein auf das Recht vertraut, um Informationssysteme sozialverträglich zu erhalten, gleicht einem Arzt, der eine einzige Arznei für alle Krankheiten und Gebrechen des Leibes und der Seele verschreibt. Dem einen wird sie nützen, einigen schaden, bei einigen schlicht unwirksam bleiben. Oder anders: die nämliche Rechtsregel kann je nach Struktur ihres Anwendungsbereiches sozial schädlich, nützlich oder indifferent sein.*⁷⁰⁵

Europa, das prinzipiell staatlichen Regelungen mehr zugeneigt ist als die US amerikanische Gesellschaft, hat durch das DSG vermehrt auch private Unternehmen darin einbezogen um in weiterer Folge daraus einen Balanceakt zwischen staatlicher Regulierung und der autonomen Möglichkeit nach informationeller Selbstbestimmung und Informationsfreiheit zu schaffen. Dies hat eigentlich so lange gut funktioniert bis der Informationstransport durch das Internet

⁷⁰⁴ Burgsdorff, Die Umsetzung der EG DS-RL, 91 fordert für D auch die Schaffung einer eigenen Rechtsaufsicht gegenüber der Kontrollstelle (Art 28 Abs 3 am Ende) und sieht die Nichtschaffung einer solchen Institution sogar als einen Verstoß gegen die RL an; aA Dammann/Simits, EG DS-RL, Art 28 Rn 5 mit Hinweis auf die Entstehungsgeschichte der RL

⁷⁰⁵ Steinmüller, in Informationssysteme für die 80er Jahre: Informationssysteme im technischen und gesellschaftlichen Wandel, Die Rolle des Rechts bei der Gestaltung von Informationssystemen, 689

fast vollständig übernommen wurde. (obwohl auch dazu gesagt werden muss, dass der Datenschutz im Internet nicht Ziel der DS-RL war und daher auch keine spezifischen Vorschriften für das Internet enthält)

Etliche Privatunternehmen haben sodann Generalklauseln so weit wie möglich ausgereizt um ihre eigenen Geschäftsinteressen zu verfolgen und Daten unter Missachtung von Datenschutz und Privatsphäre zu verarbeiten.

Einerseits ist es unbestreitbar notwendig, dass, auch vor allem jetzt in wirtschaftlich schwierigeren Zeiten, wirtschaftliche und daher auch persönliche Daten den Kreditgebern der Wirtschaft zur Verfügung stehen damit nicht die große Mehrheit die Zeche für eine kleine Minderheit bezahlt in Form von höheren Zinsen, Preisen, Geschäftspraktiken etc.

Dies jedoch hat alles unter der Einhaltung der bestehenden Gesetze zu erfolgen.

Ich bin sicher, es ist auch jedem der sich intensiver mit der Materie „Datenschutz/Kreditschutz“ befasst klar, dass dies ein sehr sensibles und diffiziles Rechtsgebiet darstellt weil erstens das Grundverständnis in der österreichischen Bevölkerung diesbezüglich noch zu wenig vorhanden ist – möglicherweise auch bewusst nicht intensiver propagiert wird - und es zweitens in Teilbereiche der „österreichischen Seele“ eindringt die viele noch immer als „heilige Kuh“ bezeichnen, nämlich der eigene finanzielle Spielraum in Form von Gehalt, Lohn, Kreditverpflichtungen, etc. und in welche in weiterer Folge auch die jeweilige soziale Stellung ausmacht.

Personen die sich in diesem Umfeld bewegen bzw. arbeiten, werden in ihrer Rolle oft als „Verhinderer“⁷⁰⁶ oder „Wachhunde“ wahrgenommen und von vielen anderen Stellen diesbezüglich kritisiert. Doch es ist genau die Aufgabe von Compliance Abteilungen, Credit Management Teams, Revision- und Audit Verantwortlichen am unternehmerischen Entscheidungsprozess teilzunehmen, einzugreifen und Rahmenbedingungen und Vorgaben auszuarbeiten und auch, wenn es notwendig die „Reißleine“ zu ziehen um Schäden für die Firma oder die Wirtschaft abzuwenden.

Seltsam dagegen erscheint die Tatsache, dass Personen bzw. Firmen als Kreditnehmer nichts daran auszusetzen haben ungezählte personenbezogene Informationen⁷⁰⁷ an ein Kreditinstitut zu übermitteln wie zB Vermögen, Gesundheit, Beruf, finanzielle und familiäre Lasten, etc.) aber es hingegen bei der geschäftlichen Beschaffung ähnlicher Daten durch eine Wirtschaftsauskunftei als unzulässige Schnüffelei und die Tätigkeit derartiger privater

⁷⁰⁶ So auch *Lubich in Baeriswyl*, (Hrsg), Perspektive Datenschutz, 55

⁷⁰⁷ Ähnlich, wenn auch nicht so in die Tiefe gehend bei der Beantragung von Bonus-, Mitglieds- und Rabattkarten u.ä. von Einzelhandelsketten

Informationssysteme als besonders gefährdet und schützenswert angesehen wird und diese auch mit einem gewissen Makel der Zwielfichtigkeit behaftet sein soll. Dies geht jedoch an der Realökonomie wie es die letzten Jahrhunderte betrieben wird, komplett vorbei.

Es muss daher nochmals deutlich gesagt werden, wer im Wirtschaftsleben steht, egal ob als Unternehmen oder Privatperson, muss damit rechnen dass seine wirtschaftlichen Daten erfasst, gespeichert und anderen Marktteilnehmer bei Bedarf zur Verfügung gestellt werden. Dies ist jedem geläufig – wenn nicht, dann ist es schon längst überfällig – und kann daher als konkludente Einwilligung in die Beschaffung und Weitergabe von wirtschaftsbezogenen Daten angesehen werden.⁷⁰⁸

Zusammenfassend kann gesagt werden, dass Österreich im Vergleich zu anderen EU- Staaten ein durchaus sehr gutes und durchdachtes Datenschutzgesetz besitzt, es aber beim Verständnis, der Anwendung und der Kontrolle mittlere bis größere Defizite aufweist. Es wird auch nichts nützen sich immer weiter reichende Verfeinerungen und juristische Konstruktionen auszudenken welche bereits aufgrund der bestehenden hohen Anforderungen nur das Vollzugsdefizit steigern, wenn es schon am Grundstock des Datenschutzbewusstseins mangelt.

Abschließen möchte ich das Thema mit folgendem Zitat der Europäischen Kommission⁷⁰⁹ dem in meinen Augen nicht mehr viel hinzuzufügen ist:

„Die rasante Entwicklung der Informations- und Kommunikationstechnologien wird [...] einen so umfassenden wirtschaftlichen und gesellschaftlichen Wandel bringen, dass bereits von einer dritten industriellen Revolution gesprochen wird.

An deren Ende wird die Informationsgesellschaft stehen.“

⁷⁰⁸ So auch Tiedemann-Sasse, Delinquenzprophylaxe, 132

⁷⁰⁹ Europäische Kommission, Die Informationsgesellschaft (1996), 3

ZUSAMMENFASSUNG

Diese Arbeit soll Spannungsverhältnis zwischen dem (Grund-)Recht auf Datenschutz und dem Bedürfnis der (kreditgebenden) Wirtschaft auf finanzielle Informationen über zukünftige Kreditnehmer (im weitesten Sinn) thematisieren. In den letzten Jahren gab es diesbezüglich auch vermehrt Beschwerden, Zeitungsartikel und das Befassen der Datenschutzkommission von betroffenen Personen und Firmen bezüglich Bonitätsauskünften und deren (negative) Auswirkungen sowohl in finanzieller als auch in sozialer Hinsicht da hiemit oft auch eine gewisse Stigmatisierung verbunden ist.

Ich habe ausgehend vom Grundrecht auf Datenschutz, EU-rechtlichen Vorgaben durch die Datenschutzrichtlinie 95/46/EU sowie deren Umsetzung im österreichischen (Verfassungs-) Recht den aktuellen Stand der Judikatur und hL aufgezeigt und analysiert.

Nachdem es bis dato im Gesetz keine genaue Regelung bezüglich Sammlung, Einholung, Beauskunftung von Bonitätsdaten gibt (abgesehen von allgemeinen Regelungen im DSG 2000) habe ich nun diesen Bereich gesetzesübergreifend untersucht und glaube auch sodann zu einer klaren Aussage bezüglich der Zulässigkeit oder auch Unzulässigkeit gekommen zu sein. Da dieses Thema auch in der Öffentlichkeit immer wieder für Empörung, Verwunderung und Erstaunen sorgt und ich in meinen bisherigen Nachforschungen sehr viele divergierende (Rechts-)meinungen und diffuse Ansichten gelesen und gehört habe, wurde es an der Zeit sich diesem Thema einmal ausführlich zu widmen und danach Klarheit in diese Thematik zu bringen. Ich habe jedoch nicht nur die Kategorie der „harten“ Bonitätskriterien bearbeitet sondern auch „weiche“ Bonitätskriterien mit einbezogen deren Entscheidungsgrundlagen für Außenstehende noch mehr Unverständnis hervorriefen.

Als Anschauungsbeispiele habe ich den Aufbau und die Arbeitsweise bei zwei großen Firmen welche in Österreich in diesem Bereich tätig sind und deren Inanspruchnahme durch fast alle Branchen verläuft, dargestellt.

Hiebei handelt es sich um den Kreditschutzverband (von 1870) welcher folgende Bonitätsdatenbanken betreibt:

- Info Datenbank (Firmen und Selbständige)
- KKE (**K**leink**k**redit**k**ataster**e**videnz - Privatpersonen)

- WKE (**W**aren**k**redite**e**videnz - Privatpersonen)
- „UKV“ Liste (Liste der „**u**nerwünschten **K**ontoverbindungen)

sowie um eine in Österreich relativ neu gegründete Firma – *Deltavista GmbH* welche sehr stark im Privatkundenbereich tätig ist und z.B. von fast allen Mobilfunkfirmen und Versandhäusern als deren Datenlieferant verwendet wird. Die Auskünfte dieser Firma kommen aus ganz verschiedenen Datenquellen und sowohl die Datenaufbereitung als auch Abfragemöglichkeiten und Ergebnisse stellen eine „kleine Revolution“ in der Bonitätsprüfung in Österreich dar.

Als Literatur werde ich mich an Artikel in Fachzeitschriften (Recht der Wirtschaft, Österreichisches Bankarchiv, Ecolex, Österreichische Juristenzeitung (ÖJZ). etc.) sowie einschlägige Lehrbücher und Fachliteratur z.B. von *Duschanek, Jahnel, Wiederin, Pawlikowky, V. Mayer-Schönberger*, usw. orientieren und deren Meinung mit meinen Erkenntnissen analysieren, vergleichen, zitieren und verarbeiten.

Weiters werde ich mich auch mit dem (volks-) wirtschaftlichen Aspekt dieses Thema befassen und deren Auswirkungen in Bezug auf die Insolvenzstatistik der letzten Jahren.

Es gibt mittlerweile auch schon einige richtungsweisende Erkenntnisse der DSK sowie Gerichtsurteile welche ich in meine Untersuchung einbezogen habe und daraus einen klaren Trend in der Rechtssprechung erkannt zu haben und dies auch gesetzlich fundieren zu können.

Aber auch die Argumente von erklärten Gegnern dieser Art von Auskünften habe ich berücksichtigt und auf deren gesetzliche Grundlage hin untersucht und in meiner Arbeit behandelt.

Auch das „beinahe nur“ österreichische Kuriosum des Bankgeheimnisses spielt hier eine nicht unbeträchtliche Rolle und erfordert eine genauere Betrachtung und Analyse.

SUMMARY

This work should broach the issue to the tense relationship between the (fundamental) right of data protection and the demand of the lending economy for financial information about future debtors (in the broadest sense).

In the last years, there have been a lot of complaints, articles in newspapers and also different cases have been brought to the attention of the Austrian Data Protection Committee of involved persons and companies about creditworthiness related information and their financial and social implications as there is sometimes also a certain stigmatization involved.

I have therefore beginning with the fundamental law of privacy, the requirements of the EU directive 95/46/EU and their implementation in the Austrian Law system reviewed, analysed and pointed out the actual prevailing case law and legal opinion.

Until now there is no exact regulation in the Austrian law system about data gathering, storing, provision of information about creditworthiness related information (except some common regulations in the Data Protection Act 2000). Therefore I have examined different fields of law and I assume that overall I could make a clear statement regarding the legitimacy or inadmissibility about this common business practices. As this topic always causes outrage, astonishment and surprise in the public, I found a lot of different law opinions and views during my investigations and it was urgently needed to immerse deeply in this matter and make a clear statement after all. I have not only aimed at “hard” credit criteria but also involved “soft” credit criteria and its basis of decision-making which is sometimes much more unclear to outsiders.

For example I have shown the construction and operation of two big companies in Austria which operate exactly in this field of activity.

Here it concerns the *Kreditschutzverband* (of 1870) which operates the following credit rating data bases:

- Info data base (companies and self employed)
- KKE (Kleinkreditkatasterevidenz – private people)

- WKE (consumption credit evidence – private people)
- UKV list (list of the unwanted bank accounts)

as well in Austria a relative new founded company called “*Deltavista*” which operates mainly in the private customer field and is used by almost all mobile phone and mail-order companies as its data provider. The information of this company comes from different data sources and as well the data preparation as well from the enquiry possibilities has caused “a small revolution” in the credit rating in Austria.

As literature I used articles in speciality journals (right of economy, Austrian bank archives, Ecolex, Austrian lawyer newspaper (ÖJZ) etc.) as well as in relevant legal text books and technical literature e.g. *Duschanek, Jahnel, Wiederin, Pawlikowky, V. Mayer-Schönberger*, etc. oriented and of their opinion with my realizations have been analyzed, compared, quoted and processed.

I have also pointed out the economic side of this topic regarding the consequences in the insolvency statistics in the past few years.

Meanwhile there have been a lot of trend-setting findings of the Austrian Data Protection Commission and verdicts of different Austrian law courts which I have included in my examination and I assume that there is a concrete tendency in the jurisdiction in Austria which can be supported legally.

But I have also considered arguments of professed opponents regarding this kind of financial information and examined their legal basis.

Also the almost unique curiosity of the Austrian banking confidentiality plays an important role in this system and needs a closer look and analysis.

LEBENS LAUF

Geboren am 28. Juni 1968 in Wien

1974 – 1978	Privatvolksschule der Piaristen in 1080 Wien
1978 – 1982	Privatgymnasium Strebersdorf in 1210 Wien
1982 – 1987	HAK V der Wr. Kaufmannschaft in 1210 Wien
20. Juni 1987	Reifeprüfung
1987 – 1988	Ableistung des Präsenzdienstes
1988 – 2003	Angestellter bei zwei Kreditkartenunternehmungen im Bereich Bonitätsprüfung, Inkasso, Betrugsbekämpfung Aufbau und Leitung der Abteilung Bonitätsprüfung bei zwei Mobilfunkunternehmen in Österreich
5. Oktober 2005	Sponsion zum Magister der Rechtswissenschaften (Mag.iur)
2005 – 2007	Verantwortlicher Credit Controller bei einem weltweit operativ tätigen Papierkonzern
ab 10/07	Studium zum Doktor der Rechtswissenschaften (Dr. iur)
Hobbies:	div. Sportarten (Mountainbiken, Snowboarden, Schwimmen, Tauchen, Beachvolleyball,...) (Auslands-)Reisen

L I T E R A T U R V E R Z E I C H N I S

<i>Apathy/Iro/Koziol</i>	Österreichisches Bankvertragsrecht ²
<i>Baeriswyl, Bruno</i>	Perspektive Datenschutz
<i>Barthel, Thomas</i>	Gefährdet die Informationstechnologie unsere Freiheit Datenschutz ist Bürgerrecht
<i>Bäumler, Helmut</i>	Datenschutz der Dritten Generation
<i>Berka, Walter</i>	Geheimnisschutz – Datenschutz – Informationsschutz im Lichte der Verfassung in <i>Eilmansberger</i> , Geheimnisschutz, Datenschutz, Informationsschutz
<i>Born, Christian</i>	Schadenersatz bei Datenschutzverstößen
<i>Burgsdorff, Christoph von</i>	Die Umsetzung der EG-Datenschutzrichtlinie im nicht-öffentlichen Bereich
<i>Dammann/Simitis</i>	EG-Datenschutzrichtlinie
<i>Dohr, Walter/(Pollirer/Weiss)</i>	Datenschutzgesetz
<i>Duschaneck, Alfred</i>	Datenschutz in der Wirtschaft: Grundfragen der Anwendung des DSG im Unternehmensbereich Datenschutz in der Wirtschaft Grundrechte für Europa Datenschutzgesetz 2000 Datenschutzgesetz (in <i>Korinek/Holubek</i> Grundrechte III)
<i>Ehmann(Eugen)/Helfrich</i>	EG-Datenschutzrichtlinie (Kurzkommentar)
<i>Ehrenzweig, Armin</i>	System des österreichischen Privatrechts ² I+II

<i>Thomas Eilmansberger u.a.</i>	Geheimnisschutz – Datenschutz - Informationsschutz (Studiengesellschaft für Wirtschaft und Recht)
<i>Ganßauge, Klaus</i>	Datenverarbeitung und -nutzung von Kreditwürdigkeitsdaten durch fremdnützige Verarbeiter
<i>Gola, Peter</i>	Betrieblicher Datenschutz
<i>Hohmann, Harald</i>	Freiheitssicherung durch Datenschutz
<i>Iro, Gert (Koziol, Helmut)</i>	Allgemeine Bedingungen für Bankgeschäfte (Kommentar)
<i>Jabornegg, Peter</i>	Kommentar zum HGB (1997+1999) Das Bankgeheimnis in <i>Jabornegg/Strasser/Floretta</i>
<i>Jahnel, Dietmar</i>	Aktuelle Fragen des Datenschutzrechts (2007) Das Grundrecht auf Datenschutz nach dem DSG 2000 (in FS <i>Schäffer</i>) Datenschutzrecht und E-Government (2008)
<i>Knyrim, Rainer</i>	Datenschutzrecht
<i>Korinek, Karl/Holubek</i>	Grundrechte II
<i>Koziol-Welser</i>	Grundriss des Bürgerlichen Recht I + II (13. Aufl)
<i>Koziol, Helmut</i>	Österreichisches Haftpflichtrecht I ³ +II ²
<i>Miller, Margret J.</i>	Credit reporting systems and the international economy
<i>Mayer-Schönberger, Viktor</i>	Datenschutzgesetz 2000 Information und Recht
<i>Oppitz, Martin</i>	Bankgeheimnis in <i>Eilmansberger</i> , Geheimnisschutz, Datenschutz, Informationsschutz
<i>Pawlikowsky, Gerhart J.</i>	Datenschutz
<i>Reimer, Sebastian</i>	Verfassungs- und europarechtliche Überlegungen zur

	datenschutzrechtlichen Zustimmung in <i>Jahnel</i> , Aktuelle Fragen des Datenschutzrechts
<i>Rummel, Peter</i>	Kommentar zum ABGB ³ I-II
<i>Ruppe, Hans Georg</i>	Geheimnisschutz im Wirtschaftsleben
<i>Schinnagl, Andreas</i>	Datenschutz – Wissen und Skepsis hinsichtlich der Erhebung und Verarbeitung personenbezogener Daten
<i>Schinnerer/Avancini</i>	Bankverträge ³ I-III
<i>Schwimann, Michael</i>	Praxiskommentar zum ABGB I-VII
<i>Tiedemann, Klaus</i>	Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft
<i>Wächter, Michael</i>	Datenschutz im Unternehmen
<i>Weber, Rolf H.</i>	Daten und Datenbanken
<i>Weitenbacher, Mario</i>	Datenschutz in Banken in Hinblick auf den Beitritt Österreichs zur Europäischen Gemeinschaft
<i>Weitenbacher, Zahra</i>	Datenschutz in Österreichs Banken
<i>Wesely, Karl</i>	Spannungsverhältnisse zwischen Datenschutz und betriebswirtschaftlichen Dispositionen
<i>Wiederin, Ewald</i>	Privatsphäre und Überwachungsstaat Art. 8 EMRK (in <i>Korinek/Holubek</i> , Grundrechte III)
<i>Wittmann, Heinz</i>	Datenschutzrecht im Unternehmen

A N H A N G I

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)

(NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) (CELEX-Nr.: 395L0046)
StF: BGBl. I Nr. 165/1999

Änderung

idF:

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81. BR: 6458 AB 6459 S. 681.)

BGBl. I Nr. 13/2005 (NR: GP XXII IA 515/A AB 821 S. 96. BR: AB 7228 S. 719.)

BGBl. I Nr. 2/2008 (1. BVRBG) (NR: GP XXIII RV 314 AB 370 S. 41. BR: 7799 AB 7830 S. 751.)

Präambel/Promulgationsklausel

Inhaltsverzeichnis

Artikel 1 (Verfassungsbestimmung)

§ 1 Grundrecht auf Datenschutz

§ 2 Zuständigkeit

§ 3 Räumlicher Anwendungsbereich

Artikel 2

1. Abschnitt: Allgemeines

§ 4 Definitionen

§ 5 Öffentlicher und privater Bereich

2. Abschnitt: Verwendung von Daten

§ 6 Grundsätze

§ 7 Zulässigkeit der Verwendung von Daten

§ 8 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 9 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 10 Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 11 Pflichten des Dienstleisters

§ 12 Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 13 Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

3. Abschnitt: Datensicherheit

§ 14 Datensicherheitsmaßnahmen

§ 15 Datengeheimnis

4. Abschnitt: Publizität der Datenverarbeitungen

§ 16 Datenverarbeitungsregister

§ 17 Meldepflicht des Auftraggebers

§ 18 Aufnahme der Verarbeitung

§ 19 Notwendiger Inhalt der Meldung

§ 20 Prüfungs- und Verbesserungsverfahren

§ 21 Registrierung

§ 22 Richtigstellung des Registers

§ 23 Pflicht zur Offenlegung nichtmeldepflichtiger Datenanwendungen

§ 24 Informationspflicht des Auftraggebers

§ 25 Pflicht zur Offenlegung der Identität des Auftraggebers

5. Abschnitt: Die Rechte des Betroffenen

§ 26 Auskunftrecht

§ 27 Recht auf Richtigstellung oder Löschung

§ 28 Widerspruchsrecht

§ 29 Die Rechte des Betroffenen bei Verwendung nur indirekt personenbezogener Daten

6. Abschnitt: Rechtsschutz

§ 30 Kontrollbefugnisse der Datenschutzkommission

§ 31 Beschwerde an die Datenschutzkommission

§ 32 Anrufung der Gerichte

§ 33 Schadenersatz

§ 34 Gemeinsame Bestimmungen

7. Abschnitt: Kontrollorgane

§ 35 Datenschutzkommission und Datenschutzrat

§ 36 Zusammensetzung der Datenschutzkommission

§ 37 Weisungsfreiheit der Datenschutzkommission

§ 38 Organisation und Geschäftsführung der Datenschutzkommission

§ 39 Beschlüsse der Datenschutzkommission

§ 40 Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds

§ 41 Einrichtung und Aufgaben des Datenschutzrates

§ 42 Zusammensetzung des Datenschutzrates

§ 43 Vorsitz und Geschäftsführung des Datenschutzrates

§ 44 Sitzungen und Beschlußfassung des Datenschutzrates

8. Abschnitt: Besondere Verwendungszwecke von Daten

§ 45 Private Zwecke

§ 46 Wissenschaftliche Forschung und Statistik

§ 47 Zur Verfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 48 Publizistische Tätigkeit

§ 48a. Verwendung von Daten im Katastrophenfall

9. Abschnitt: Besondere Verwendungsarten von Daten

§ 49 Automatisierte Einzelentscheidungen

§ 50 Informationsverbundsysteme

10. Abschnitt: Strafbestimmungen

§ 51 Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 52 Verwaltungsstrafbestimmung

11. Abschnitt: Übergangs- und Schlussbestimmungen

§ 53 Befreiung von Gebühren, Verwaltungsabgaben und von Kostenersatz

§ 54 Mitteilungen an die anderen Mitgliedstaaten der Europäischen Union und an die Europäische Kommission

§ 55 Feststellungen der Europäischen Kommission

§ 56 Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 57 Sprachliche Gleichbehandlung

§ 58 Manuelle Dateien

§ 59 Umsetzungshinweis

§ 60 Inkrafttreten

§ 61 Übergangsbestimmungen

§ 62 Verordnungserlassung

§ 63 Verweisungen

§ 64 Vollziehung

Text

Artikel 1

(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, 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. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher

1. 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;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

Bestimmungen

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) 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. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, dass Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

Verfassungsbestimmung

Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Beachte

Verfassungsbestimmung

Räumlicher Anwendungsbereich

§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

Artikel 2

1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. „Auftraggeber“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Ständesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;
5. „Dienstleister“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z 8);
6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

7. „Datenanwendung“ (früher: „Datenverarbeitung“): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), 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);
8. „Verwenden von Daten“: jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. „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 einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z 12) von Daten;
10. „Ermitteln von Daten“: das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
11. „Überlassen von Daten“: die Weitergabe von Daten vom Auftraggeber an einen Dienstleister;
12. „Übermitteln von Daten“: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
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;
14. „Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

Öffentlicher und privater Bereich

§ 5. (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

2. Abschnitt

Verwendung von Daten

Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen
2. Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der
5. Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen 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.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder
2. rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, 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 eingehalten werden.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
 2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
 3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
 4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder
 5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
 6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
- 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 ist; im letztgenannten Fall gilt § 48a Abs. 3.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
 2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
- sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden
3. berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der

Daten bewirkt, oder

7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
9. des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik
10. gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen
11. Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der
12. Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten
13. Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 10. (1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, dass die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzkommission zur Auffassung, dass die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden;
1. insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;

alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen
2. für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;

weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den
3. Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann;

- sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem
4. Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunft-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;

nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten
5. enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;

dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der
6. Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Mitgliedstaaten der Europäischen Union ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

(3) Darüberhinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen
3. ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§

48) übermittelt werden oder

5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des
6. Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder
9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfaßt sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder
2. zur Wahrung eines lebenswichtigen Interesses einer Person

notwendig und so dringlich ist, dass die gemäß § 13 erforderliche Genehmigung der Datenschutzkommission nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzkommission umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muß darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 13 Abs. 5 an den inländischen Dienstleister - vorliegen, dass er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder

der Auftraggeber glaubhaft macht, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden.
2. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein.

(3) Im Genehmigungsverfahren haben Auftraggeber des öffentlichen Bereichs auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.

(4) Bei meldepflichtigen Datenanwendungen hat die Datenschutzkommission eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen und die Erteilung der Genehmigung im Datenverarbeitungsregister (§ 16) anzumerken.

(5) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen. Der Auftraggeber hat der Datenschutzkommission mitzuteilen, aus welcher seiner meldepflichtigen Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Datenverarbeitungsregister anzumerken.

(6) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich gilt hinsichtlich der Pflicht zur Einholung von Genehmigungen nach Abs. 1 als Datenverkehr mit dem Ausland.

(7) Hat der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung festgestellt, dass für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gemäß Abs. 2 Z 1 zutreffen, tritt an die Stelle der Verpflichtung zur Einholung einer Genehmigung die Pflicht zur Anzeige an die Datenschutzkommission. Die Datenschutzkommission hat binnen sechs Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

3. Abschnitt

Datensicherheit

Datensicherheitsmaßnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen
3. Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät
6. durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere
7. Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, dass dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis

§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter - das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis - haben 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).

(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

4. Abschnitt

Publizität der Datenanwendungen

Datenverarbeitungsregister

§ 16. (1) Bei der Datenschutzkommission ist ein Register der Datenanwendungen zum Zweck der Prüfung ihrer Rechtmäßigkeit und zum Zweck der Information der Betroffenen eingerichtet.

(2) Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er Betroffener ist, und soweit nicht überwiegende

schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen. Es ist die Möglichkeit vorzusehen, eine Meldung (§§ 17 und 19) auf automationsunterstütztem Wege vorzunehmen.

Meldepflicht des Auftraggebers

§ 17. (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
 2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder
 3. nur indirekt personenbezogene Daten enthalten oder
 4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
 5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
- einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die
6. Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
 2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
 3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
 4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
 5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten
- von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

Aufnahme der Verarbeitung

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie

1. sensible Daten enthalten oder
 2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
 3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
 4. in Form eines Informationsverbundsystems durchgeführt werden sollen,
- erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden.

Notwendiger Inhalt der Meldung

§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten:

- den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines
1. allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
- die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden
5. Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzkommission notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

(2) Wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, kann der Bundeskanzler durch Verordnung Musteranwendungen festlegen. Meldungen über Datenanwendungen, die inhaltlich einer Musteranwendung entsprechen, müssen nur folgendes enthalten:

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und
2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und
3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

(3) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, dass Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte nach diesem Bundesgesetz keine hinreichende Information darüber gewinnen können, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

Prüfungs- und Verbesserungsverfahren

§ 20. (1) Die Datenschutzkommission hat alle Meldungen binnen zwei Monaten zu prüfen. Kommt sie hiebei zur Auffassung, dass eine Meldung im Sinne des § 19 Abs. 3 mangelhaft ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen.

(2) Liegt wegen wesentlicher Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen durch die gemeldete Datenanwendung Gefahr im Verzug vor, so hat die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG vorläufig zu untersagen.

(3) Bei Datenanwendungen, die gemäß § 18 Abs. 2 der Vorabkontrolle unterliegen, ist gleichzeitig mit einem allfälligen Auftrag zur Verbesserung darüber abzusprechen, ob die Verarbeitung bereits aufgenommen werden darf oder ob dies mangels Nachweises ausreichender Rechtsgrundlagen für die gemeldete Datenanwendung nicht zulässig ist.

(4) Wird einem Verbesserungsauftrag nicht fristgerecht entsprochen, so hat die Datenschutzkommission die Registrierung mit Bescheid abzulehnen; andernfalls gilt die Meldung als ursprünglich richtig eingebracht.

(5) Wird innerhalb von zwei Monaten nach Erstattung der Meldung kein Auftrag zur Verbesserung erteilt, gilt die Meldepflicht als erfüllt. Bei Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, darf die Verarbeitung aufgenommen werden.

(6) Im Registrierungsverfahren haben Auftraggeber des öffentlichen Bereichs auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren die Zulässigkeit der Registrierung ergeben hat oder
2. zwei Monate nach Einlangung der Meldung bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 1 erteilt wurde oder
3. der Auftraggeber die verlangten Verbesserungen fristgerecht vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 Abs. 2 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszeuges mitzuteilen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

Richtigstellung des Registers

§ 22. (1) Streichungen und Änderungen im Datenverarbeitungsregister sind auf Antrag des Eingetragenen oder in den Fällen der Abs. 2 und 4 von Amts wegen durchzuführen.

(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist von Amts wegen die Streichung aus dem Register anzuordnen.

(3) Änderungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Bescheid zu verfügen.

(4) Werden der Datenschutzkommission andere als die in Abs. 2 bezeichneten Umstände bekannt, die den Verdacht der Mangelhaftigkeit einer Registrierung im Sinne des § 19 Abs. 3 oder der rechtswidrigen Unterlassung einer Meldung begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.

Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen

§ 23. (1) Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen, welche Standardanwendungen sie tatsächlich vornehmen.

(2) Nicht-meldepflichtige Datenanwendungen sind der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben gemäß § 30 offenzulegen.

Informationspflicht des Auftraggebers

§ 24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

(2) Über Abs. 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder
wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für
3. Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adreßdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind.

Pflicht zur Offenlegung der Identität des Auftraggebers

§ 25. (1) Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodass den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne dass diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hierbei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.

5. Abschnitt

Die Rechte des Betroffenen

Auskunftsrecht

§ 26. (1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
 2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
 3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
 4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
 5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten
- ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

(3) Der Betroffene hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen:

Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.

(8) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat der Betroffene ein Recht auf Auskunft in dem Umfang, in dem ein Einsichtsrecht besteht. Für das Verfahren der Einsichtnahme gelten die näheren Regelungen der das öffentliche Buch oder Register einrichtenden Gesetze.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 4 Z 4, dritter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zulässt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, dass die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschantrag durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und lässt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hievon in geeigneter

Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
 2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschanträge von Betroffenen
- durch Bundesgesetz nicht anderes bestimmt ist.

Widerspruchsrecht

§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

§ 29. Die durch die §§ 26 bis 28 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

6. Abschnitt

Rechtsschutz

Kontrollbefugnisse der Datenschutzkommission

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes oder eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. ein Verfahren zur Überprüfung der Registrierung gemäß § 22 Abs. 4 einleiten, oder
2. Strafanzeige nach §§ 51 oder 52 erstatten, oder
3. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der
4. Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzkommission

§ 31. (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 26 durch den Auftraggeber einer

Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

(3) Bei Gefahr im Verzug kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde nach Abs. 2 die weitere Verwendung von Daten zur Gänze oder teilweise untersagen oder auch - bei Streitigkeiten über die Richtigkeit von Daten - dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.

(4) Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtet oder gelöscht wurden.

Anrufung der Gerichte

§ 32. (1) Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstrebenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

(5) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.

(6) Die Datenschutzkommission hat, wenn ein Betroffener es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von Betroffenen geboten ist, einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

Schadenersatz

§ 33. (1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

(3) Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. Dasselbe gilt für die Haftungsbefreiung des Dienstleisters. Für den Fall eines Mitverschuldens des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 ABGB.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 32 Abs. 4.

Gemeinsame Bestimmungen

§ 34. (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind abzuweisen.

(2) Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 sowie Schadenersatzansprüche nach § 33 können nicht nur auf die Verletzung der Vorschriften dieses Bundesgesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates

der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 3 im Inland anzuwenden sind.

(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Inland gemäß § 3 nach der Rechtsordnung eines anderen Mitgliedstaats der Europäischen Union zu beurteilen, so kann die Datenschutzkommission im Falle ihrer Befassung die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen Amtshilfe zu leisten.

Beachte

Abs. 2: Verfassungsbestimmung

7. Abschnitt

Kontrollorgane

Datenschutzkommission und Datenschutzrat

§ 35. (1) Zur Wahrung des Datenschutzes sind nach den näheren Bestimmungen dieses Bundesgesetzes - unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte - die Datenschutzkommission und der Datenschutzrat berufen.

(2) (Verfassungsbestimmung) Die Datenschutzkommission übt ihre Befugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung aus.

Zusammensetzung der Datenschutzkommission

§ 36. (1) Die Datenschutzkommission besteht aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Die Mitglieder müssen rechtskundig sein. Ein Mitglied muß dem Richterstand angehören.

(2) Die Vorbereitung des Vorschlages der Bundesregierung für die Bestellung der Mitglieder der Datenschutzkommission obliegt dem Bundeskanzler. Er hat dabei Bedacht zu nehmen auf:

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

Alle vorgeschlagenen Personen sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen.

(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbeamten vorzuschlagen.

(4) Für jedes Mitglied ist ein Ersatzmitglied zu bestellen. Das Ersatzmitglied tritt bei Verhinderung des Mitglieds an dessen Stelle. Die Funktionsperiode des Ersatzmitglieds endet mit der Funktionsperiode des Mitglieds; für den Fall der vorzeitigen Beendigung der Funktionsperiode des Mitglieds gilt Abs. 8.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschlussgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt.

(7) Auf die Ersatzmitglieder sind die Abs. 2, 3, 5 und 6 wie auf Mitglieder anzuwenden.

(8) Scheidet ein Mitglied wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so wird das betreffende Ersatzmitglied (Abs. 4) Mitglied der Datenschutzkommission bis zum Ablauf der Funktionsperiode des ausgeschiedenen Mitglieds. Unter Anwendung der Abs. 2 und 3 ist für diese Zeit ein neues Ersatzmitglied zu bestellen. Scheidet ein Ersatzmitglied vorzeitig aus, ist unverzüglich ein neues Ersatzmitglied zu bestellen.

(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine dem Zeit- und Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.

Weisungsfreiheit der Datenschutzkommission

§ 37. (1) Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.

(2) Die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission.

Beachte

Abs. 1: Verfassungsbestimmung

Organisation und Geschäftsführung der Datenschutzkommission

§ 38. (1) (Verfassungsbestimmung) Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfaßt auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren gemäß § 20 Abs. 2 oder § 22 Abs. 3. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.

(2) Für die Unterstützung in der Geschäftsführung der Datenschutzkommission hat der Bundeskanzler eine Geschäftsstelle einzurichten und die notwendige Sach- und Personalausstattung bereitzustellen.

(3) Die Datenschutzkommission ist vor Erlassung von Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen.

(4) Die Datenschutzkommission hat spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Der Bericht ist dem Bundeskanzler zur Kenntnis zu übermitteln.

Beschlüsse der Datenschutzkommission

§ 39. (1) Die Datenschutzkommission ist bei Anwesenheit aller sechs Mitglieder beschlußfähig. Für den Fall der Verhinderung eines Mitglieds gilt § 36 Abs. 4.

(2) Das richterliche Mitglied führt den Vorsitz.

(3) Für einen gültigen Beschluß der Datenschutzkommission ist die Zustimmung der Mehrheit der abgegebenen Stimmen notwendig. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig.

(4) Entscheidungen der Datenschutzkommission von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzkommission unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

Wirkung von Bescheiden der Datenschutzkommission und desgeschäftsführenden Mitglieds

§ 40. (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 20 Abs. 2 oder § 22 Abs. 3 in Verbindung mit § 38 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Eine Vorstellung gegen einen gemäß § 22 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Die Anrufung des

Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist außer in den Fällen des Abs. 1 zulässig. Dies gilt auch für die in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs in jenen Fällen, in welchen ihnen gemäß § 13 Abs. 3 oder § 20 Abs. 6 Parteistellung zukommt oder durch Gesetz ausdrücklich ein Beschwerderecht an den Verwaltungsgerichtshof eingeräumt wurde.

(3) Bescheide, mit welchen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen und tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 ergangenen Kundmachung des Bundeskanzlers, nicht mehr bestehen.

(4) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so hat dieser mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.

Einrichtung und Aufgaben des Datenschutzrates

§ 41. (1) Beim Bundeskanzleramt ist ein Datenschutzrat eingerichtet.

(2) Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen;
2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;
3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;
hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
4. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;
5. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.
- 6.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung des Datenschutzrates

§ 42. (1) Dem Datenschutzrat gehören an:

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

1. Vertreter und von jeder anderen im Hauptausschuß des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden. Bei Mandatsgleichheit der beiden im Nationalrat am stärksten vertretenen Parteien entsendet jede dieser Parteien drei Vertreter;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

(2) Die in Abs. 1 Z 3, 4 und 5 genannten Vertreter sollen berufliche Erfahrung auf dem Gebiet der Informatik und des Datenschutzes haben.

(3) Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen.

(4) Dem Datenschutzrat können Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind, nicht angehören.

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird.

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

Vorsitz und Geschäftsführung des Datenschutzes

§ 43. (1) Der Datenschutzrat gibt sich mit Beschluß eine Geschäftsordnung.

(2) Der Datenschutzrat hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert - unbeschadet des § 42 Abs. 5 - fünf Jahre. Wiederbestellungen sind zulässig.

(3) Die Geschäftsführung des Datenschutzes obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzes gebunden.

Sitzungen und Beschlußfassung des Datenschutzes

§ 44. (1) Die Sitzungen des Datenschutzes werden vom Vorsitzenden nach Bedarf einberufen. Begehrt ein Mitglied die Einberufung einer Sitzung, so hat der Vorsitzende die Sitzung so einzuberufen, dass sie binnen vier Wochen stattfinden kann.

(2) Zu den Sitzungen kann der Vorsitzende nach Bedarf Sachverständige zuziehen.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig.

(4) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen.

(5) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - außer im Fall der gerechtfertigten Verhinderung - teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hievon unverzüglich das Ersatzmitglied zu verständigen.

(6) Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen nicht zu.

(7) Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich.

(8) Die Mitglieder des Datenschutzrates, die anwesenden Mitglieder der Datenschutzkommission und die zur Sitzung gemäß Abs. 2 zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

8. Abschnitt

Besondere Verwendungszwecke von Daten

Private Zwecke

§ 45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit § 7 Abs. 2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

Wissenschaftliche Forschung und Statistik

§ 46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für den Auftraggeber nur indirekt personenbezogen sind.

Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten, die nicht öffentlich zugänglich sind, nur

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.

(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist zu erteilen, wenn

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

Sollen sensible Daten übermittelt werden, muß ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muß gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

(2) Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
 - a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
 - b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzkommission gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder
2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke erfolgen soll.

(4) Die Datenschutzkommission hat die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

(5) Die übermittelten Adreßdaten dürfen ausschließlich für den genehmigten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adreßdaten notwendigen Verarbeitungen vorgenommen werden.

Publizistische Tätigkeit

§ 48. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes verwenden, sind von den

einfachgesetzlichen Bestimmungen des vorliegenden Bundesgesetzes nur die §§ 4 bis 6, 10, 11, 14 und 15 anzuwenden.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

(3) Im übrigen gelten die Bestimmungen des Mediengesetzes, insbesondere seines dritten Abschnitts über den Persönlichkeitsschutz.

Verwendung von Daten im Katastrophenfall

§ 48a. (1) Auftraggeber des öffentlichen Bereiches sind im Katastrophenfall ermächtigt, Daten zu verwenden, 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 ist. Zu diesem Zweck sind auch Hilfsorganisationen (Abs. 6) nach Maßgabe der ihnen zukommenden Aufgaben und rechtlichen Befugnis ermächtigt, Daten zu verwenden. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung in Form der Teilnahme an einem Informationsverbundsystem erfolgen. Wer rechtmäßig über Daten verfügt, darf diese an Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen übermitteln, sofern diese die Daten zur Bewältigung der Katastrophe für die genannten Zwecke benötigen. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

(2) Eine Überlassung oder Übermittlung von Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke notwendig ist. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung durch Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen in Form der Teilnahme an einem Informationsverbundsystem, an dem auch ausländische Auftraggeber beteiligt sind, erfolgen. Die Übermittlung erkenntnisdienlicher und sensibler Daten zu Identifizierungszwecken an ein derartiges System darf erst stattfinden, wenn auf Grund von Erhebungen konkrete Anhaltspunkte dafür vorliegen, dass die vermisste Person verstorben sein dürfte. Daten, die für sich allein den Betroffenen strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Übermittlung von Daten Angehöriger darf nur in pseudonymisierter Form erfolgen. Daten dürfen in Staaten ohne angemessenes Datenschutzniveau nur übermittelt oder überlassen werden, wenn der Auftraggeber auf Grund schriftlicher Vereinbarungen mit dem Empfänger oder auf Grund schriftlicher Zusagen des Empfängers oder, wenn dies nach den Umständen nicht oder nicht in angemessener Zeit möglich ist, durch Erteilung von Auflagen an den Empfänger davon ausgehen kann, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Eine Übermittlung oder Überlassung hat dann zu unterbleiben, wenn Grund zur Annahme besteht, dass der Empfänger nicht für den gebotenen Schutz der Geheimhaltungsinteressen der Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen des Auftraggebers missachten werde. Während der Dauer der Katastrophensituation entfällt im Hinblick auf § 12 Abs. 3 Z 3 die Genehmigungspflicht. Die Datenschutzkommission ist von den veranlassten Übermittlungen und Überlassungen und den näheren Umständen des Anlass gebenden Sachverhaltes jedoch unverzüglich zu

verständigen. Die Datenschutzkommission kann zum Schutz der Betroffenenrechte Datenübermittlungen oder -überlassungen untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

(3) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Auftraggeber ermächtigt, dem Anfragenden Daten über die Reise in das und aus dem Katastrophengebiet, Aufenthaltsdaten im Katastrophengebiet sowie Daten über den Stand der Ausforschung von betroffenen Personen zu übermitteln, wenn der Angehörige folgende Daten bekannt gibt:

1. Vor- und Zuname, Geburtsdatum sowie Wohnadresse der tatsächlich oder vermutlich von der Katastrophe betroffenen Person und
2. seinen Vor- und Zunamen, sein Geburtsdatum, seine Wohnadresse und sonstige Erreichbarkeit sowie seine Angehörigeneigenschaft zur betroffenen Person.

Bestehen Zweifel an der Angehörigeneigenschaft und können diese durch Überprüfungen nicht ausgeräumt werden, ist ein Nachweis der Identität und Angehörigeneigenschaft notwendig.

(4) Über Abs. 3 hinaus dürfen nahen Angehörigen von Auftraggebern des öffentlichen Bereiches und Hilfsorganisationen Daten einschließlich sensibler Daten über tatsächlich oder vermutlich unmittelbar von der Katastrophe betroffene Personen nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Auskunft zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger sind verpflichtet, die Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen bei der Überprüfung der Daten gemäß Abs. 3 und der Angehörigenbeziehung zu unterstützen. Behörden sind ermächtigt, die zur Überprüfung dieser Angaben notwendigen Daten im Wege der Amtshilfe zu ermitteln und für diesen Zweck zu verwenden.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten und Lebensgefährten der Betroffenen zu verstehen. Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann.

(7) Alle Datenverwendungen sind im Sinne des § 14 Abs. 2 Z 7 zu protokollieren.

(8) Die Zulässigkeit von Datenverwendungen auf der Grundlage anderer in den §§ 8 und 9 genannter Tatbestände bleibt unberührt.

9. Abschnitt

Besondere Verwendungsarten von Daten

Automatisierte Einzelentscheidungen

§ 49. (1) Niemand darf 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, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

(2) Abweichend von Abs. 1 darf eine Person einer ausschließlich automationsunterstützt erzeugten Entscheidung unterworfen werden, wenn

1. dies gesetzlich ausdrücklich vorgesehen ist oder
die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und
2. dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder
die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen -
3. beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen - garantiert wird.

(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen.

Informationsverbundsysteme

§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, dass kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne dass eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten auf den Betreiber übertragen werden. Soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber den Betroffenen und den für die Vollziehung dieses Bundesgesetzes zuständigen Behörden nur wirksam, wenn er - auf Grund einer entsprechenden Meldung an die Datenschutzkommission - aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. (1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 18 890 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere
2. Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht;
5. sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 48a verschafft.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 9 445 Euro zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 erfüllt zu haben oder
2. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder
3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder

4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.

11. Abschnitt

Übergangs- und Schlußbestimmungen

Befreiung von Gebühren, Abgaben und vom Kostenersatz

§ 53. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 21 Abs. 3 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

(2) Für Abschriften aus dem Datenverarbeitungsregister, die ein Betroffener zur Verfolgung seiner Rechte benötigt, ist kein Kostenersatz zu verlangen.

Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

§ 54. (1) Von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, hat der Bundeskanzler anläßlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen.

(2) Die Datenschutzkommission hat den anderen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission mitzuteilen, in welchen Fällen

1. keine Genehmigung für den Datenverkehr in ein Drittland erteilt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 1 nicht als gegeben erachtet wurden;
2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 2 als gegeben erachtet wurden.

Feststellungen der Europäischen Kommission

§ 55. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen

bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über

1. das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder
 2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland
- ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 2 Abs. 3 BGBlG, BGBl. Nr. 660/1996, kundzumachen.

Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 56. Der Präsident des Nationalrats ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß Art. 30 B-VG übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Nationalrats vorgenommen werden. Der Präsident trifft Vorsorge dafür, dass im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

Sprachliche Gleichbehandlung

§ 57. Soweit in diesem Artikel auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Manuelle Dateien

§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, dass die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.

Umsetzungshinweis

§ 59. Mit diesem Bundesgesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S 31, umgesetzt.

Inkrafttreten

§ 60. (1) (Anm.: Durch Art. 2 § 2 Abs. 1 Z 24 und Abs. 2 Z 71, BGBl. I Nr. 2/2008, als nicht mehr geltend festgestellt.)

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(3) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

Beachte

Abs. 4: Verfassungsbestimmung

Übergangsbestimmungen

§ 61. (1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.

(2) Soweit nach der neuen Rechtslage eine Genehmigung für die Übermittlung von Daten ins Ausland erforderlich ist, muß für Übermittlungen, für die eine Genehmigung vor Inkrafttreten dieses Bundesgesetzes erteilt wurde, eine Genehmigung vor dem 1. Jänner 2003 neu beantragt werden. Wird der Antrag rechtzeitig gestellt, dürfen solche Übermittlungen bis zur rechtskräftigen Entscheidung über den Genehmigungsantrag fortgeführt werden.

(3) Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes stattgefunden haben, sind, soweit es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts handelt, nach der Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts zu beurteilen; soweit es sich um die Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrundezulegen. Ein strafbarer Tatbestand ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(4) (Verfassungsbestimmung) Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke notwendig sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 ausreichenden gesetzlichen Grundlage bis 31. Dezember 2007 vorgenommen werden, in den Fällen des § 17 Abs. 3 Z 1 bis 3 jedoch bis zur Erlassung von bundesgesetzlichen Regelungen über die Aufgaben und Befugnisse in diesen Bereichen.

(5) Manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, sind, soweit sie schon im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden. Dasselbe gilt für automationsunterstützte Datenanwendungen gemäß § 17 Abs. 3, für die durch die nunmehr geltende Rechtslage die Meldepflicht neu eingeführt wurde.

(6) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Datenschutzkommission übernimmt für den Zeitraum von sechs Monaten ab Inkrafttreten dieses Gesetzes die Funktion der Datenschutzkommission gemäß § 35.

(7) Soweit in einzelnen Vorschriften Verweise auf das Datenschutzgesetz, BGBl. Nr. 565/1978, enthalten sind, gelten diese bis zu ihrer Anpassung an dieses Bundesgesetz sinngemäß weiter.

Verordnungserlassung

§ 62. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 63. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 64. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung oder den Landesregierungen obliegt, der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereiches betraut.

ANHANG II

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 Datenverkehr⁷¹⁰

Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 - 0050

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 100a,

auf Vorschlag der Kommission (1),

nach Stellungnahme des Wirtschafts- und Sozialausschusses (2),

gemäß dem Verfahren des Artikels 189b des Vertrags (3),

in Erwägung nachstehender Gründe:

(1) Die Ziele der Gemeinschaft, wie sie in dem durch den Vertrag über die Europäische Union geänderten Vertrag festgelegt sind, bestehen darin, einen immer engeren Zusammenschluss der europäischen Völker zu schaffen, engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossenen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.

⁷¹⁰ Allfällige Änderungen in der Schreibweise wurden von mir aufgrund Anpassung an die neue Rechtsschreibung durchgeführt

(3) Für die Errichtung und das Funktionieren des Binnenmarktes, der gemäß Artikel 7a des Vertrags den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleisten soll, ist es nicht nur erforderlich, dass personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können, sondern auch, dass die Grundrechte der Personen gewahrt werden.

(4) Immer häufiger werden personenbezogene Daten in der Gemeinschaft in den verschiedenen Bereichen wirtschaftlicher und sozialer Tätigkeiten verarbeitet. Die Fortschritte der Informationstechnik erleichtern die Verarbeitung und den Austausch dieser Daten beträchtlich.

(5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Artikel 7a des Vertrags ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschaftsrechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaats durchführen zu können.

(6) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Telekommunikationsnetze in der Gemeinschaft erfordern und erleichtern den grenzüberschreitenden Verkehr personenbezogener Daten.

(7) Das unterschiedliche Niveau des Schutzes der Rechte und Freiheiten von Personen, insbesondere der Privatsphäre, bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaats in das Gebiet eines anderen Mitgliedstaats verhindern. Dieses unterschiedliche Schutzniveau kann somit ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und die Erfüllung des Auftrags der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden verhindern. Dieses unterschiedliche Schutzniveau ergibt sich aus der Verschiedenartigkeit der einzelstaatlichen Rechts- und Verwaltungsvorschriften.

(8) Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerlässlich. Insbesondere unter Berücksichtigung der großen Unterschiede, die gegenwärtig zwischen den einschlägigen einzelstaatlichen Rechtsvorschriften bestehen, und der Notwendigkeit, die Rechtsvorschriften der Mitgliedstaaten zu koordinieren, damit der grenzüberschreitende Fluss personenbezogener Daten kohärent und in Übereinstimmung mit dem Ziel des Binnenmarktes im Sinne des Artikels 7a des Vertrags geregelt wird, läßt sich dieses für den Binnenmarkt grundlegende Ziel nicht allein durch das Vorgehen der Mitgliedstaaten verwirklichen. Deshalb ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich.

(9) Die Mitgliedstaaten dürfen aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen. Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an. Innerhalb dieses Spielraums können unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann.

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

(11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

(12) Die Schutzprinzipien müssen für alle Verarbeitungen personenbezogener Daten gelten, sobald die Tätigkeiten des für die Verarbeitung Verantwortlichen in den Anwendungsbereich des Gemeinschaftsrechts fallen. Auszunehmen ist die Datenverarbeitung, die von einer natürlichen Person in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten - wie zum Beispiel Schriftverkehr oder Führung von Anschriftenverzeichnissen - vorgenommen wird

(13) Die in den Titeln V und VI des Vertrags über die Europäische Union genannten Tätigkeiten, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im Bereich des Strafrechts betreffen, fallen unbeschadet der Verpflichtungen der Mitgliedstaaten gemäß Artikel 56 Absatz 2 sowie gemäß den Artikeln 57 und 100a des Vertrags zur Gründung der Europäischen Gemeinschaft nicht in den Anwendungsbereich des Gemeinschaftsrechts. Die Verarbeitung personenbezogener Daten, die zum Schutz des wirtschaftlichen Wohls des Staates erforderlich ist, fällt nicht unter diese Richtlinie, wenn sie mit Fragen der Sicherheit des Staates zusammenhängt.

(14) In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muss diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden.

(15) Die Verarbeitung solcher Daten wird von dieser Richtlinie nur erfasst, wenn sie automatisiert erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen.

(16) Die Verarbeitung von Ton- und Bilddaten, wie bei der Videoüberwachung, fällt nicht unter diese Richtlinie, wenn sie für Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder der Tätigkeiten des Staates im Bereich des Strafrechts oder anderen Tätigkeiten erfolgt, die nicht unter das Gemeinschaftsrecht fallen.

(17) Bezüglich der Verarbeitung von Ton- und Bilddaten für journalistische, literarische oder künstlerische Zwecke, insbesondere im audiovisuellen Bereich, finden die Grundsätze dieser Richtlinie gemäß Artikel 9 eingeschränkt Anwendung.

(18) Um zu vermeiden, dass einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird, müssen auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaats angewandt werden. Es ist angebracht, auf die Verarbeitung, die von einer Person, die dem in dem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen unterstellt ist, vorgenommen werden, die Rechtsvorschriften dieses Staates anzuwenden.

(19) Eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich. Wenn der Verantwortliche im Hoheitsgebiet mehrerer Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muss er vor allem zu Vermeidung von Umgehungen sicherstellen, dass jede dieser Niederlassungen die Verpflichtungen einhält, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, das auf ihre jeweiligen Tätigkeiten anwendbar ist.

(20) Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Rechte und Pflichten tatsächlich eingehalten werden.

(21) Diese Richtlinie berührt nicht die im Strafrecht geltenden Territorialitätsregeln.

(22) Die Mitgliedstaaten können in ihren Rechtsvorschriften oder bei der Durchführung der Vorschriften zur Umsetzung dieser Richtlinie die allgemeinen Bedingungen präzisieren, unter denen die Verarbeitungen rechtmäßig sind. Insbesondere nach Artikel 5 in Verbindung mit den Artikeln 7 und 8 können die Mitgliedstaaten neben den allgemeinen Regeln besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen und für die verschiedenen Datenkategorien gemäß Artikel 8 vorsehen.

(23) Die Mitgliedstaaten können den Schutz von Personen sowohl durch ein allgemeines Gesetz zum Schutz von Personen bei der Verarbeitung personenbezogener Daten als auch durch

gesetzliche Regelungen für bestimmte Bereiche, wie zum Beispiel die statistischen Ämter, sicherstellen.

(24) Diese Richtlinie berührt nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen.

(25) Die Schutzprinzipien finden zum einen ihren Niederschlag in den Pflichten, die den Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung verantwortlichen Stellen obliegen; diese Pflichten betreffen insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Daten zu erhalten, ihre Berichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können.

(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht.

(27) Datenschutz muss sowohl für automatisierte als auch für nicht automatisierte Verarbeitungen gelten. In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden. Bei manuellen Verarbeitungen erfasst diese Richtlinie lediglich Dateien, nicht jedoch unstrukturierte Akten. Insbesondere muss der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein, die einen leichten Zugriff auf die Daten ermöglichen. Nach der Definition in Artikel 2 Buchstabe c) können die Mitgliedstaaten die Kriterien zur Bestimmung der Elemente einer strukturierten Sammlung personenbezogener Daten sowie die verschiedenen Kriterien zur Regelung des Zugriffs zu einer solchen Sammlung festlegen. Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich dieser Richtlinie.

(28) Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Sie hat den angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein.

(29) Die Weiterverarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, wenn der Mitgliedstaat geeignete Garantien vorsieht. Diese Garantien müssen insbesondere ausschließen, dass die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.

(30) Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf der Einwilligung der betroffenen Person beruht oder notwendig ist im Hinblick auf den Abschluss oder die Erfüllung eines für die betroffene Person bindenden Vertrags, zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder wenn sie im Interesse einer anderen Person erforderlich ist, vorausgesetzt, dass die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Um den Ausgleich der in Frage stehenden Interessen unter Gewährleistung eines effektiven Wettbewerbs sicherzustellen, können die Mitgliedstaaten insbesondere die Bedingungen näher bestimmen, unter denen personenbezogene Daten bei rechtmäßigen Tätigkeiten im Rahmen laufender Geschäfte von Unternehmen und anderen Einrichtungen an Dritte weitergegeben werden können. Ebenso können sie die Bedingungen festlegen, unter denen personenbezogene Daten an Dritte zum Zweck der kommerziellen Werbung oder der Werbung von Wohltätigkeitsverbänden oder anderen Vereinigungen oder Stiftungen, z. B. mit politischer Ausrichtung, weitergegeben werden können, und zwar unter Berücksichtigung der Bestimmungen dieser Richtlinie, nach denen betroffene Personen ohne Angabe von Gründen und ohne Kosten Widerspruch gegen die Verarbeitung von Daten, die sie betreffen, erheben können.

(31) Die Verarbeitung personenbezogener Daten ist ebenfalls als rechtmäßig anzusehen, wenn sie erfolgt, um ein für das Leben der betroffenen Person wesentliches Interesse zu schützen.

(32) Es ist nach einzelstaatlichem Recht festzulegen, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht oder das Privatrecht fallende Person, wie beispielsweise eine Berufsvereinigung, handeln soll.

(33) Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen, dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot müssen ausdrücklich vorgesehen werden bei spezifischen Notwendigkeiten, insbesondere wenn die Verarbeitung dieser Daten für gewisse auf das Gesundheitswesen bezogene Zwecke von Personen vorgenommen wird, die nach dem einzelstaatlichen Recht dem Berufsgeheimnis unterliegen, oder wenn die Verarbeitung für berechnete Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, deren Ziel es ist, die Ausübung von Grundfreiheiten zu ermöglichen.

(34) Die Mitgliedstaaten können, wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien vorsehen in Bereichen wie dem öffentlichen Gesundheitswesen und der sozialen Sicherheit - insbesondere hinsichtlich der Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen -, der wissenschaftlichen Forschung und der öffentlichen Statistik. Die Mitgliedstaaten müssen jedoch geeignete besondere Garantien zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.

(35) Die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im Völkerrecht niedergelegte Zwecke von staatlich anerkannten Religionsgesellschaften erfolgt ebenfalls im Hinblick auf ein wichtiges öffentliches Interesse.

(36) Wenn es in bestimmten Mitgliedstaaten zum Funktionieren des demokratischen Systems gehört, dass die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen eines wichtigen öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.

(37) Für die Verarbeitung personenbezogener Daten zu journalistischen, literarischen oder künstlerischen Zwecken, insbesondere im audiovisuellen Bereich, sind Ausnahmen von bestimmten Vorschriften dieser Richtlinie vorzusehen, soweit sie erforderlich sind, um die Grundrechte der Person mit der Freiheit der Meinungsäußerung und insbesondere der Freiheit, Informationen zu erhalten oder weiterzugeben, die insbesondere in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und der Grundfreiheiten garantiert ist, in Einklang zu bringen. Es obliegt deshalb den Mitgliedstaaten, unter Abwägung der Grundrechte Ausnahmen und Einschränkungen festzulegen, die bei den allgemeinen Maßnahmen zur Rechtmäßigkeit der Verarbeitung von Daten, bei den Maßnahmen zur Übermittlung der Daten in Drittländer sowie hinsichtlich der Zuständigkeiten der Kontrollstellen erforderlich sind, ohne dass jedoch Ausnahmen bei den Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorzusehen sind. Ferner sollte mindestens die in diesem Bereich zuständige Kontrollstelle bestimmte nachträgliche Zuständigkeiten erhalten, beispielsweise zur regelmäßigen Veröffentlichung eines Berichts oder zur Befassung der Justizbehörden.

(38) Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.

(39) Bestimmte Verarbeitungen betreffen Daten, die der Verantwortliche nicht unmittelbar bei der betroffenen Person erhoben hat. Des weiteren können Daten rechtmäßig an Dritte weitergegeben werden, auch wenn die Weitergabe bei der Erhebung der Daten bei der betroffenen Person nicht vorgesehen war. In diesen Fällen muss die betroffene Person zum Zeitpunkt der Speicherung der Daten oder spätestens bei der erstmaligen Weitergabe der Daten an Dritte unterrichtet werden.

(40) Diese Verpflichtung erübrigt sich jedoch, wenn die betroffene Person bereits unterrichtet ist. Sie besteht auch nicht, wenn die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist oder wenn die Unterrichtung der betroffenen Person unmöglich ist oder unverhältnismäßigen Aufwand erfordert, was bei Verarbeitungen für historische, statistische oder wissenschaftliche Zwecke der Fall sein kann. Diesbezüglich können die Zahl der betroffenen Personen, das Alter der Daten und etwaige Ausgleichsmaßnahmen in Betracht gezogen werden.

(41) Jede Person muss ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, haben, damit sie sich insbesondere von der Richtigkeit dieser Daten und der Zulässigkeit ihrer Verarbeitung überzeugen kann. Aus denselben Gründen muss jede Person außerdem das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne des Artikels 15 Absatz 1, besitzen. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insbesondere das Urheberrecht zum

Schutz von Software, berühren. Dies darf allerdings nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

(42) Die Mitgliedstaaten können die Auskunfts- und Informationsrechte im Interesse der betroffenen Person oder zum Schutz der Rechte und Freiheiten Dritter einschränken. Zum Beispiel können sie vorsehen, dass Auskunft über medizinische Daten nur über ärztliches Personal erhalten werden kann.

(43) Die Mitgliedstaaten können Beschränkungen des Auskunfts- und Informationsrechts sowie bestimmter Pflichten des für die Verarbeitung Verantwortlichen vorsehen, soweit dies beispielsweise für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, für zwingende wirtschaftliche oder finanzielle Interessen eines Mitgliedstaats oder der Union oder für die Ermittlung und Verfolgung von Straftaten oder von Verstößen gegen Standesregeln bei reglementierten Berufen erforderlich ist. Als Ausnahmen und Beschränkungen sind Kontroll-, Überwachungs- und Ordnungsfunktionen zu nennen, die in den drei letztgenannten Bereichen in bezug auf öffentliche Sicherheit, wirtschaftliches oder finanzielles Interesse und Strafverfolgung erforderlich sind. Die Erwähnung der Aufgaben in diesen drei Bereichen lässt die Zulässigkeit von Ausnahmen und Einschränkungen aus Gründen der Sicherheit des Staates und der Landesverteidigung unberührt.

(44) Die Mitgliedstaaten können aufgrund gemeinschaftlicher Vorschriften gehalten sein, von den das Auskunftsrecht, die Information der Personen und die Qualität der Daten betreffenden Bestimmungen dieser Richtlinie abzuweichen, um bestimmte der oben genannten Zweckbestimmungen zu schützen.

(45) Auch wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung aufgrund eines öffentlichen Interesses, der Ausübung hoheitlicher Gewalt oder der Interessen eines einzelnen sein können, sollte doch jede betroffene Person das Recht besitzen, aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch dagegen einzulegen, dass die sie betreffenden Daten verarbeitet werden. Die Mitgliedstaaten können allerdings innerstaatliche Bestimmungen vorsehen, die dem entgegenstehen.

(46) Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern. Die Mitgliedstaaten haben dafür Sorge zu tragen, dass der für die Verarbeitung Verantwortliche diese Maßnahmen einhält. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(47) Wird eine Nachricht, die personenbezogene Daten enthält, über Telekommunikationsdienste oder durch elektronische Post übermittelt, deren einziger Zweck darin besteht, Nachrichten dieser Art zu übermitteln, so gilt in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten. Jedoch gelten die

Personen, die diese Dienste anbieten, in der Regel als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind.

(48) Die Meldeverfahren dienen der Offenlegung der Zweckbestimmungen der Verarbeitungen sowie ihrer wichtigsten Merkmale mit dem Zweck der Überprüfung ihrer Vereinbarkeit mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

(49) Um unangemessene Verwaltungsformalitäten zu vermeiden, können die Mitgliedstaaten bei Verarbeitungen, bei denen eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht zu erwarten ist, von der Meldepflicht absehen oder sie vereinfachen, vorausgesetzt, dass diese Verarbeitungen den Bestimmungen entsprechen, mit denen der Mitgliedstaat die Grenzen solcher Verarbeitungen festgelegt hat. Eine Befreiung oder eine Vereinfachung kann ebenso vorgesehen werden, wenn ein vom für die Verarbeitung Verantwortlichen benannter Datenschutzbeauftragter sicherstellt, dass eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen durch die Verarbeitung nicht zu erwarten ist. Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können.

(50) Die Befreiung oder Vereinfachung kann vorgesehen werden für Verarbeitungen, deren einziger Zweck das Führen eines Registers ist, das gemäß einzelstaatlichem Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

(51) Die Vereinfachung oder Befreiung von der Meldepflicht entbindet jedoch den für die Verarbeitung Verantwortlichen von keiner der anderen sich aus dieser Richtlinie ergebenden Verpflichtungen.

(52) In diesem Zusammenhang ist die nachträgliche Kontrolle durch die zuständigen Stellen im Allgemeinen als ausreichende Maßnahme anzusehen.

(53) Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen - oder aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen. Es obliegt den Mitgliedstaaten, derartige Risiken in ihren Rechtsvorschriften aufzuführen, wenn sie dies wünschen.

(54) Bei allen in der Gesellschaft durchgeführten Verarbeitungen sollte die Zahl der Verarbeitungen mit solchen besonderen Risiken sehr beschränkt sein. Die Mitgliedstaaten müssen für diese Verarbeitungen vorsehen, dass vor ihrer Durchführung eine Vorabprüfung durch die Kontrollstelle oder in Zusammenarbeit mit ihr durch den Datenschutzbeauftragten vorgenommen wird. Als Ergebnis dieser Vorabprüfung kann die Kontrollstelle gemäß einzelstaatlichem Recht eine Stellungnahme abgeben oder die Verarbeitung genehmigen. Diese Prüfung kann auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

(55) Für den Fall der Missachtung der Rechte der betroffenen Personen durch den für die Verarbeitung Verantwortlichen ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen. Mögliche Schäden, die den Personen aufgrund einer unzulässigen Verarbeitung entstehen, sind von dem für die Verarbeitung Verantwortlichen zu ersetzen, der von seiner Haftung befreit werden kann, wenn er nachweist, dass der Schaden ihm nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt. Unabhängig davon, ob es sich um eine Person des Privatrechts oder des öffentlichen Rechts handelt, müssen Sanktionen jede Person treffen, die die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht einhält.

(56) Grenzüberschreitender Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels notwendig. Der in der Gemeinschaft durch diese Richtlinie gewährte Schutz von Personen steht der Übermittlung personenbezogener Daten in Drittländer, die ein angemessenes Schutzniveau aufweisen, nicht entgegen. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlung oder eine Kategorie von Übermittlungen zu beurteilen.

(57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.

(58) Ausnahmen von diesem Verbot sind unter bestimmten Voraussetzungen vorzusehen, wenn die betroffene Person ihre Einwilligung erteilt hat oder die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel bei internationalem Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind. Ebenso kann eine Übermittlung aus einem gesetzlich vorgesehenen Register erfolgen, das der öffentlichen Einsichtnahme oder der Einsichtnahme durch Personen mit berechtigtem Interesse dient. In diesem Fall sollte eine solche Übermittlung nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Ist ein Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, so sollte die Übermittlung nur auf Antrag dieser Person oder nur dann erfolgen, wenn diese Person die Adressaten der Übermittlung sind.

(59) Besondere Maßnahmen können getroffen werden, um das unzureichende Schutzniveau in einem Drittland auszugleichen, wenn der für die Verarbeitung Verantwortliche geeignete Sicherheiten nachweist. Außerdem sind Verfahren für die Verhandlungen zwischen der Gemeinschaft und den betreffenden Drittländern vorzusehen.

(60) Übermittlungen in Drittstaaten dürfen auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften erfolgen, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gemäß Artikel 8, erlassen haben.

(61) Die Mitgliedstaaten und die Kommission müssen in ihren jeweiligen Zuständigkeitsbereichen die betroffenen Wirtschaftskreise ermutigen, Verhaltensregeln auszuarbeiten, um unter Berücksichtigung der Besonderheiten der Verarbeitung in bestimmten Bereichen die Durchführung dieser Richtlinie im Einklang mit den hierfür vorgesehenen einzelstaatlichen Bestimmungen zu fördern.

(62) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.

(63) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden, sowie Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in dem Mitgliedstaat beizutragen, dem sie unterstehen.

(64) Die Behörden der verschiedenen Mitgliedstaaten werden einander bei der Wahrnehmung ihrer Aufgaben unterstützen müssen, um sicherzustellen, dass die Schutzregeln in der ganzen Europäischen Union beachtet werden.

(65) Auf Gemeinschaftsebene ist eine Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten einzusetzen, die ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Unter Berücksichtigung dieses besonderen Charakters hat sie die Kommission zu beraten und insbesondere zur einheitlichen Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften beizutragen.

(66) Für die Übermittlung von Daten in Drittländern ist es zur Anwendung dieser Richtlinie erforderlich, der Kommission Durchführungsbefugnisse zu übertragen und ein Verfahren gemäß den Bestimmungen des Beschlusses 87/373/EWG des Rates (4) festzulegen.

(67) Am 20. Dezember 1994 wurde zwischen dem Europäischen Parlament, dem Rat und der Kommission ein Modus vivendi betreffend die Maßnahmen zur Durchführung der nach dem Verfahren des Artikels 189b des EG-Vertrag erlassenen Rechtsakte vereinbart.

(68) Die in dieser Richtlinie enthaltenen Grundsätze des Schutzes der Rechte und Freiheiten der Personen und insbesondere der Achtung der Privatsphäre bei der Verarbeitung personenbezogener Daten können - besonders für bestimmte Bereiche - durch spezifische Regeln ergänzt oder präzisiert werden, die mit diesen Grundsätzen in Einklang stehen.

(69) Den Mitgliedstaaten sollte eine Frist von längstens drei Jahren ab Inkrafttreten ihrer Vorschriften zur Umsetzung dieser Richtlinie eingeräumt werden, damit sie die neuen einzelstaatlichen Vorschriften fortschreitend auf alle bereits laufenden Verarbeitungen anwenden können. Um eine kosteneffiziente Durchführung dieser Vorschriften zu erleichtern, wird den Mitgliedstaaten eine weitere Frist von zwölf Jahren nach Annahme dieser Richtlinie eingeräumt, um die Anpassung bestehender manueller Dateien an bestimmte Vorschriften dieser Richtlinie sicherzustellen. Werden in solchen Dateien enthaltene Daten während dieser erweiterten Umsetzungsfrist manuell verarbeitet, so sollten die Dateien zum Zeitpunkt der Verarbeitung mit diesen Vorschriften in Einklang gebracht werden.

(70) Die betroffene Person braucht nicht erneut ihre Einwilligung zu geben, damit der Verantwortliche nach Inkrafttreten der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie eine Verarbeitung sensibler Daten fortführen kann, die für die Erfüllung eines in freier Willenserklärung geschlossenen Vertrags erforderlich ist und vor Inkrafttreten der genannten Vorschriften mitgeteilt wurde.

(71) Diese Richtlinie steht den gesetzlichen Regelungen eines Mitgliedstaats im Bereich der geschäftsmäßigen Werbung gegenüber in seinem Hoheitsgebiet ansässigen Verbrauchern nicht entgegen, sofern sich diese gesetzlichen Regelungen nicht auf den Schutz der Person bei der Verarbeitung personenbezogener Daten beziehen.

(72) Diese Richtlinie erlaubt bei der Umsetzung der mit ihr festgelegten Grundsätze die Berücksichtigung des Grundsatzes des öffentlichen Zugangs zu amtlichen Dokumenten -

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand der Richtlinie

(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

b) "Verarbeitung personenbezogener Daten" ("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;

c) "Datei mit personenbezogenen Daten" ("Datei") jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese

Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;

d) "für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;

e) "Auftragsverarbeiter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

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

g) "Empfänger" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;

h) "Einwilligung der betroffenen Person" jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

Artikel 3

Anwendungsbereich

(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

- die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.

Artikel 4

Anwendbares einzelstaatliches Recht

(1) Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erläßt, auf alle Verarbeitungen personenbezogener Daten an,

a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;

b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;

c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

(2) In dem in Absatz 1 Buchstabe c) genannten Fall hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

KAPITEL II ALLGEMEINE BEDINGUNGEN FÜR DIE RECHTMÄSSIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 5

Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

ABSCHNITT I GRUNDSÄTZE IN BEZUG AUF DIE QUALITÄT DER DATEN

Artikel 6

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

ABSCHNITT II GRUNDSÄTZE IN BEZUG AUF DIE ZULÄSSIGKEIT DER VERARBEITUNG VON DATEN

Artikel 7

Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

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

c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;

e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;

f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, 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 Absatz 1 geschützt sind, überwiesen.

ABSCHNITT III BESONDERE KATEGORIEN DER VERARBEITUNG

Artikel 8

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.

(2) Absatz 1 findet in folgenden Fällen keine Anwendung:

a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden;

oder

b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist;

oder

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;

oder

d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr

unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden;

oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

(3) Absatz 1 gilt nicht, wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

(4) Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.

(5) Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.

Die Mitgliedstaaten können vorsehen, dass Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.

(6) Die in den Absätzen 4 und 5 vorgesehenen Abweichungen von Absatz 1 sind der Kommission mitzuteilen.

(7) Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.

Artikel 9

Verarbeitung personenbezogener Daten und Meinungsfreiheit

Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.

ABSCHNITT IV INFORMATION DER BETROFFENEN PERSON

Artikel 10

Information bei der Erhebung personenbezogener Daten bei der betroffenen Person

Die Mitgliedstaaten sehen vor, dass die Person, bei der die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

- a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,
 - b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,
 - c) weitere Informationen, beispielsweise betreffend
 - die Empfänger oder Kategorien der Empfänger der Daten,
 - die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,
 - das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,
- sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Artikel 11

Informationen für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden

(1) Für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, sehen die Mitgliedstaaten vor, dass die betroffene Person bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

- a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,
- b) Zweckbestimmungen der Verarbeitung,
- c) weitere Informationen, beispielsweise betreffend
 - die Datenkategorien, die verarbeitet werden,

- die Empfänger oder Kategorien der Empfänger der Daten,

- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(2) Absatz 1 findet - insbesondere bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung - keine Anwendung, wenn die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. In diesen Fällen sehen die Mitgliedstaaten geeignete Garantien vor.

ABSCHNITT V AUSKUNFTSRECHT DER BETROFFENEN PERSON

Artikel 12

Auskunftsrecht

Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen folgendes zu erhalten:

a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten

- die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;

- eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;

- Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne von Artikel 15 Absatz 1;

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;

c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b) durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern

sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

ABSCHNITT VI AUSNAHMEN UND EINSCHRÄNKUNGEN

Artikel 13

Ausnahmen und Einschränkungen

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

a) die Sicherheit des Staates;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;

e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;

f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

(2) Vorbehaltlich angemessener rechtlicher Garantien, mit denen insbesondere ausgeschlossen wird, dass die Daten für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden, können die Mitgliedstaaten in Fällen, in denen offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht, die in Artikel 12 vorgesehenen Rechte gesetzlich einschränken, wenn die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet werden oder personenbezogen nicht länger als erforderlich lediglich zur Erstellung von Statistiken aufbewahrt werden.

ABSCHNITT VII WIDERSPRUCHSRECHT DER BETROFFENEN PERSON

Artikel 14

Widerspruchsrecht der betroffenen Person

Die Mitgliedstaaten erkennen das Recht der betroffenen Person an,

a) zumindest in den Fällen von Artikel 7 Buchstaben e) und f) jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen Widerspruch einlegen zu können, dass sie betreffende Daten verarbeitet werden; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen;

b) auf Antrag kostenfrei gegen eine vom für die Verarbeitung Verantwortlichen beabsichtigte Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen oder vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor deren erstmaliger Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden und ausdrücklich auf das Recht hingewiesen zu werden, kostenfrei gegen eine solche Weitergabe oder Nutzung Widerspruch einlegen zu können.

Die Mitgliedstaaten ergreifen die erforderlichen Maßnahmen, um sicherzustellen, dass die betroffenen Personen vom Bestehen des unter Buchstabe b) Unterabsatz 1 vorgesehenen Rechts Kenntnis haben.

Artikel 15

Automatisierte Einzelentscheidungen

(1) Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

(2) Die Mitgliedstaaten sehen unbeschadet der sonstigen Bestimmungen dieser Richtlinie vor, dass eine Person einer Entscheidung nach Absatz 1 unterworfen werden kann, sofern diese

a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags ergeht und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen - garantiert wird oder

b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

ABSCHNITT VIII VERTRAULICHKEIT UND SICHERHEIT DER VERARBEITUNG

Artikel 16

Vertraulichkeit der Verarbeitung

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

Artikel 17

Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(2) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.

(3) Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere folgendes vorgesehen ist:

- Der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen;
- die in Absatz 1 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

(4) Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in Bezug auf Maßnahmen nach Absatz 1 schriftlich oder in einer anderen Form zu dokumentieren.

ABSCHNITT IX MELDUNG

Artikel 18

Pflicht zur Meldung bei der Kontrollstelle

(1) Die Mitgliedstaaten sehen eine Meldung durch den für die Verarbeitung Verantwortlichen oder gegebenenfalls seinen Vertreter bei der in Artikel 28 genannten Kontrollstelle vor, bevor eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen durchgeführt wird.

(2) Die Mitgliedstaaten können eine Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht nur in den folgenden Fällen und unter folgenden Bedingungen vorsehen:

- Sie legen für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung fest, und/oder

- der für die Verarbeitung Verantwortliche bestellt entsprechend dem einzelstaatlichen Recht, dem er unterliegt, einen Datenschutzbeauftragten, dem insbesondere folgendes obliegt:

- die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen,

- die Führung eines Verzeichnisses mit den in Artikel 21 Absatz 2 vorgesehenen Informationen über die durch den für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung,

um auf diese Weise sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht beeinträchtigt werden.

(3) Die Mitgliedstaaten können vorsehen, dass Absatz 1 keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines Register ist, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

(4) Die Mitgliedstaaten können die in Artikel 8 Absatz 2 Buchstabe d) genannten Verarbeitungen von der Meldepflicht ausnehmen oder die Meldung vereinfachen.

(5) Die Mitgliedstaaten können die Meldepflicht für nicht automatisierte Verarbeitungen von personenbezogenen Daten generell oder in Einzelfällen vorsehen oder sie einer vereinfachten Meldung unterwerfen.

Artikel 19

Inhalt der Meldung

(1) Die Mitgliedstaaten legen fest, welche Angaben die Meldung zu enthalten hat. Hierzu gehört zumindest folgendes:

a) Name und Anschrift des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

b) die Zweckbestimmung(en) der Verarbeitung;

c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

d) die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;

e) eine geplante Datenübermittlung in Drittländer;

f) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

(2) Die Mitgliedstaaten legen die Verfahren fest, nach denen Änderungen der in Absatz 1 genannten Angaben der Kontrollstelle zu melden sind.

Artikel 20

Vorabkontrolle

(1) Die Mitgliedstaaten legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

(2) Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muss.

(3) Die Mitgliedstaaten können eine solche Prüfung auch im Zuge der Ausarbeitung einer Maßnahme ihres Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchführen, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

Artikel 21

Öffentlichkeit der Verarbeitungen

(1) Die Mitgliedstaaten erlassen Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstelle ein Register der gemäß Artikel 18 gemeldeten Verarbeitungen führt.

Das Register enthält mindestens die Angaben nach Artikel 19 Absatz 1 Buchstaben a) bis e).

Das Register kann von jedermann eingesehen werden.

(3) Die Mitgliedstaaten sehen vor, dass für Verarbeitungen, die von der Meldung ausgenommen sind, der für die Verarbeitung Verantwortliche oder eine andere von den Mitgliedstaaten benannte Stelle zumindest die in Artikel 19 Absatz 1 Buchstaben a) bis e) vorgesehenen Angaben auf Antrag jedermann in geeigneter Weise verfügbar macht.

Die Mitgliedstaaten können vorsehen, dass diese Bestimmungen keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen von Registern ist, die gemäß den Rechts- und Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt sind und die entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen.

KAPITEL III RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 22

Rechtsbehelfe

Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.

Artikel 23

Haftung

(1) Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.

(2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

Artikel 24

Sanktionen

Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind.

KAPITEL IV ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Artikel 25

Grundsätze

(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden 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 berücksichtigt.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

(4) Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.

(5) Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gemäß Absatz 4 festgestellte Lage zu schaffen.

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

Artikel 26

Ausnahmen

(1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, dass eine Übermittlung oder eine

Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern

a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder

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

c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder

e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder

f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.

(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten über die von ihm nach Absatz 2 erteilten Genehmigungen.

Legt ein anderer Mitgliedstaat oder die Kommission einen in Bezug auf den Schutz der Privatsphäre, der Grundrechte und der Personen hinreichend begründeten Widerspruch ein, so erlässt die Kommission die geeigneten Maßnahmen nach dem Verfahren des Artikels 31 Absatz 2.

Die Mitgliedstaaten treffen die aufgrund des Beschlusses der Kommission gebotenen Maßnahmen.

(4) Befindet die Kommission nach dem Verfahren des Artikels 31 Absatz 2, dass bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Absatz 2 bieten, so treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

KAPITEL V VERHALTENSREGELN

Artikel 27

(1) Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

(2) Die Mitgliedstaaten sehen vor, dass die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können.

Die Mitgliedstaaten sehen vor, dass sich diese Stellen insbesondere davon überzeugt, dass die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Die Stelle holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint.

(3) Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, dass die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.

KAPITEL VI KONTROLLSTELLE UND GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 28

Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.

Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;

- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

Artikel 29

Datenschutzgruppe

(1) Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend "Gruppe" genannt).

Die Gruppe ist unabhängig und hat beratende Funktion.

(2) Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission.

Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.

(3) Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.

(4) Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

(5) Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

(6) Die Gruppe gibt sich eine Geschäftsordnung.

(7) Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.

Artikel 30

(1) Die Gruppe hat die Aufgabe,

a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;

b) zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;

c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;

d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.

(2) Stellt die Gruppe fest, dass sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen könnten, so teilt sie dies der Kommission mit.

(3) Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.

(4) Die Stellungnahmen und Empfehlungen der Gruppe werden der Kommission und dem in Artikel 31 genannten Ausschuss übermittelt.

(5) Die Kommission teilt der Gruppe mit, welche Konsequenzen sie aus den Stellungnahmen und Empfehlungen gezogen hat. Sie erstellt hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht.

(6) Die Gruppe erstellt jährlich einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, den sie der Kommission, dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht.

KAPITEL VII GEMEINSCHAFTLICHE DURCHFÜHRUNGSMASSNAHMEN

Artikel 31

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

(2) Der Vertreter der Kommission unterbreitet dem Ausschuss einen Entwurf der zu treffenden Maßnahmen. Der Ausschuss gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann.

Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 148 Absatz 2 des Vertrags vorgesehen ist. Bei der Abstimmung im Ausschuss werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil.

Die Kommission erlässt Maßnahmen, die unmittelbar gelten. Stimmen sie jedoch mit der Stellungnahme des Ausschusses nicht überein, werden sie von der Kommission unverzüglich dem Rat mitgeteilt. In diesem Fall gilt folgendes:

- Die Kommission verschiebt die Durchführung der von ihr beschlossenen Maßnahmen um drei Monate vom Zeitpunkt der Mitteilung an;
- der Rat kann innerhalb des im ersten Gedankenstrich genannten Zeitraums mit qualifizierter Mehrheit einen anders lautenden Beschluss fassen.

SCHLUSSBESTIMMUNGEN

Artikel 32

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen.

Wenn die Mitgliedstaaten derartige Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass Verarbeitungen, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits begonnen wurden, binnen drei Jahren nach diesem Zeitpunkt mit diesen Bestimmungen in Einklang gebracht werden.

Abweichend von Unterabsatz 1 können die Mitgliedstaaten vorsehen, dass die Verarbeitungen von Daten, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits in manuellen Dateien enthalten sind, binnen zwölf Jahren nach Annahme dieser Richtlinie mit den Artikeln 6, 7 und 8 in Einklang zu bringen sind. Die Mitgliedstaaten gestatten jedoch, dass die betroffene Person auf Antrag und insbesondere bei Ausübung des Zugangsrechts die Berichtigung, Löschung oder Sperrung von Daten erreichen kann, die unvollständig, unzutreffend oder auf eine Art und Weise aufbewahrt sind, die mit den vom für die Verarbeitung Verantwortlichen verfolgten rechtmäßigen Zwecken unvereinbar ist.

(3) Abweichend von Absatz 2 können die Mitgliedstaaten vorbehaltlich geeigneter Garantien vorsehen, dass Daten, die ausschließlich zum Zwecke der historischen Forschung aufbewahrt werden, nicht mit den Artikeln 6, 7 und 8 in Einklang gebracht werden müssen.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 33

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig, und zwar erstmals drei Jahre nach dem in Artikel 32 Absatz 1 genannten Zeitpunkt, einen Bericht über die Durchführung dieser Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei. Dieser Bericht wird veröffentlicht.

Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten.

Artikel 34

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Luxemburg am 24. Oktober 1995.

Im Namen des Europäischen Parlaments

Der Präsident

K. HÄNSCH

Im Namen des Rates

Der Präsident

L. ATIENZA SERNA

(1) ABl. Nr. C 277 vom 5. 11. 1990, S. 3, und ABl. Nr. C 311 vom 27. 11. 1992, S. 30.

(2) ABl. Nr. C 159 vom 17. 6. 1991, S. 38.

(3) Stellungnahme des Europäischen Parlaments vom 11. März 1992 (ABl. Nr. C 94 vom 13. 4. 1992, S. 198), bestätigt am 2. Dezember 1993 (ABl. Nr. C 342 vom 20. 12. 1993, S. 30).
Gemeinsamer Standpunkt des Rates vom 20. Februar 1995 (ABl. Nr. C 93 vom 13. 4. 1995, S. 1)
und Beschluß des Europäischen Parlaments vom 15. Juni 1995 (ABl. Nr. C 166 vom 3. 7. 1995).

(4) ABl. Nr. L 197 vom 18. 7. 1987, S. 33.