

Diplomarbeit

zur Erlangung des akademischen Grades
Magister der Rechtswissenschaften

an der
Rechtswissenschaftlichen Fakultät der Karl-Franzens-Universität Graz

**Schadenersatz für den Bruch des Datengeheimnisses
nach § 33 DSGVO 2000**

eingereicht bei: o.Univ.Prof.Dr. Monika Hinteregger

von: Günther Grohmann

Graz, im Mai 2003

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benützten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Graz, Mai 2003

Inhaltsverzeichnis

<u>Inhaltsverzeichnis</u>	i
<u>Abkürzungsverzeichnis</u>	iv
<u>1. Einführung</u>	1
<u>1.1 Einleitung</u>	1
<u>1.2 Was bedeutet Datenschutz?</u>	3
<u>1.3 Die Geschichte des Datenschutzes in Österreich</u>	4
<u>1.4 Exkurs: Schadenersatz im DSG 1978</u>	8
<u>2. Grundsätze des Datenschutzes</u>	9
<u>2.1 Das Grundrecht auf Datenschutz</u>	9
<u>2.2 Datenschutz und Verfassung</u>	12
<u>3. Überblick über das DSG 2000</u>	13
<u>3.1 Definitionen</u>	13
<u>3.1.1 Personenbezogene Daten</u>	13
<u>3.1.1.1 Nur indirekt personenbezogene Daten</u>	14
<u>3.1.1.2 Anonymisierte Daten</u>	15
<u>3.1.1.3 Sensible Daten</u>	16
<u>3.1.2 Betroffener</u>	16
<u>3.1.3 Auftraggeber</u>	17
<u>3.1.4 Dienstleister</u>	18
<u>3.1.5 Abgrenzung der Begriffe „Auftraggeber“ und „Dienstleister“</u>	19
<u>3.1.6 Verwenden von Daten</u>	20
<u>3.2 Der Schutz des Datengeheimnisses durch das DSG 2000</u>	20
<u>4. Schadenersatz im DSG 2000</u>	24
<u>4.1 Abgrenzung öffentlicher – privater Bereich</u>	24
<u>4.2 Allgemeines zum Schadenersatz</u>	25
<u>4.3 Schaden</u>	25
<u>4.3.1 Materielle Schäden</u>	26
<u>4.3.2 Immaterielle Schäden</u>	26
<u>4.4 Kausalität</u>	27

<u>4.5 Rechtswidrigkeit</u>	27
<u>4.5.1 Grundsätze</u>	28
<u>4.5.2 Zulässigkeit der Verwendung von Daten</u>	30
<u>4.5.3 Schutzwürdige Geheimhaltungsinteressen bei Verwendung von nicht-sensiblen Daten</u>	31
<u>4.5.4 Schutzwürdige Geheimhaltungsinteressen bei Verwendung von sensiblen Daten</u>	32
<u>4.5.5 Dienstleistung im Datenverkehr</u>	33
<u>4.5.6 Überlassung von Daten in das Ausland</u>	35
<u>4.5.7 Rechtfertigungsgründe</u>	37
<u>4.5.7.1 Notwehr</u>	37
<u>4.5.7.2 Notstand</u>	37
<u>4.5.7.3 Selbsthilfe</u>	38
<u>4.5.7.4 Einwilligung des Verletzten</u>	38
<u>4.5.8 Überblick über die Rechtswidrigkeit</u>	38
<u>4.6 Rechtswidrigkeitszusammenhang</u>	39
<u>4.7 Verschulden</u>	40
<u>4.7.1 Vorsatz und Fahrlässigkeit</u>	40
<u>4.7.2 Beweislast</u>	41
<u>4.8 Gehilfenhaftung</u>	42
<u>4.9 Mitverantwortung des Geschädigten</u>	44
<u>4.10 Immaterieller Schadenersatz</u>	45
<u>4.10.1 Rechtswidrige oder öffentlich zugängliche Verwendung</u>	46
<u>4.10.2 Die Datenarten des § 18 Abs 2 Z 1 bis 3</u>	46
<u>4.10.3 Verletzung des höchstpersönlichen Lebensbereichs</u>	47
<u>4.10.4 Bloßstellung in der Öffentlichkeit</u>	49
<u>4.10.5 Geltendmachung und Bemessung der Entschädigung</u>	52
<u>4.10.6 Zusammentreffen von mehreren Ansprüchen</u>	53
<u>4.11 Verfahrensrecht</u>	53
<u>4.11.1 Zuständigkeit</u>	53
<u>4.11.2 Nebenintervention der DSK</u>	54
<u>4.11.3 Verjährung</u>	54
<u>5. Kritische Gedanken zu § 33 DSG 2000</u>	55
<u>5.1 Verschuldensunabhängige Haftung?</u>	56
<u>5.2 Immaterielle Schäden</u>	57
<u>5.3 Legitimation zur Geltendmachung</u>	59
<u>5.4 Wortlaut des § 33 DSG 2000</u>	61
<u>5.5 Kritische Gesamtbetrachtung des § 33 DSG 2000</u>	62

<u>6. Schadenersatz für den Bruch des Datengeheimnisses im öffentlichen Bereich</u>	63
<u>7. Schlussfolgerungen</u>	65
<u>Literaturverzeichnis</u>	68
Anhang	
<u>§ 33 DSG 2000</u>	A
<u>Artikel 23 DS-RL</u>	B

Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliches Gesetzbuch JGS 946
ABI	Amtsblatt
Abs	Absatz
AG	Aktiengesellschaft
AHG	Amtshaftungsgesetz BGBl 1949/20
Art	Artikel
ÄrzteG 1998	Ärztegesetz 1998 BGBl I 1998/169
AVG	Allgemeines Verwaltungsverfahrensgesetz 1991 BGBl 51 (Wv)
BG	Bundesgesetz
BGBl	Bundesgesetzblatt
BlgNR	Beilage(-n) zu den stenographischen Protokollen des Nationalrates
BVfG	(deutsches) Bundesverfassungsgericht
BVfGE	Entscheidungen des (deutschen) Bundesverfassungsgerichts
B-VG	Bundes-Verfassungsgesetz BGBl 1930/1 (Wv)
BWG	Bankwesengesetz BGBl 1993/532
bzw	beziehungsweise
CR	„Computer und Recht“
dh	das heißt
DHG	Dienstnehmerhaftpflichtgesetz BGBl 1965/80
DSAV	Datenschutzangemessenheits-Verordnung BGBl II 1999/521
DSG 1978	Datenschutzgesetz 1978 BGBl 1978/565
DSG 2000	Datenschutzgesetz 2000 BGBl I 1999/165
DSK	Datenschutzkommission
DS-RL	Datenschutzrichtlinie der Europäischen Union RL 95/46/EG
DuD	„Zeitschrift für Datenschutz“
DVR	Datenverarbeitungsregister
ecolex	„Fachzeitschrift für Wirtschaftsrecht“
EDV	Elektronische Datenverarbeitung
EDVuR	„EDV und Recht“

EG	Europäische Gemeinschaft(en)
ErläutRV	Erläuterungen zur Regierungsvorlage
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte Zeitschrift
f	und der, die folgende
ff	und der, die folgenden
FJ	„Finanzjournal“
FN	Fußnote
gem	gemäß
GP	Gesetzgebungsperiode
HGB	Handelsgesetzbuch dRGBI 1897, 219
Hrsg	Herausgeber
HS	Halbsatz
insbes	insbesondere
iSd	im Sinne des, - der
iVm	in Verbindung mit
JAB	Justizausschussbericht
JBI	„Juristische Blätter“
JGS	Justizgesetzsammlung
JN	Jurisdiktionsnorm RGBI 1895/111
JUS	„Jus-Extra“
KAKuG	Krankenanstalten- und Kuranstaltengesetz BGBI 1957/1
Kfz	Kraftfahrzeug
KG	Kommanditgesellschaft
LG	Landesgericht
LGBISt	Landesgesetzblatt Steiermark
lit	litera (Buchstabe)
MedG	Mediengesetz BGBI 1981/314
MeldeG	Meldegesetz 1991 BGBI 1992/9
MR	„Medien und Recht“
MRK	(Europäische) Menschenrechtskonvention BGBI 1958/210
NJW	„Neue Juristische Wochenschrift“
NR	Nationalrat

ÖBI	„Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht“
OGH	Oberster Gerichtshof
OHG	offene Handelsgesellschaft
OLG	Oberlandesgericht
ÖNorm	Österreichische Norm
OrgHG	Organhaftpflichtgesetz BGBl 1967/181
PC	Personal Computer
Pkt	Punkt
RDV	„Recht der Datenverarbeitung“
RdW	„Österreichisches Recht der Wirtschaft“
RIS	Rechtsinformationssystem des Bundes
RL	Richtlinie der EU
Rs	Rechtssache
RV	Regierungsvorlage
Rz	Randzahl
S	Satz
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen BGBl III 1997/90
Sess	Session
Slg	Sammlung der Rechtsprechung des EuGH
SozSi	„Soziale Sicherheit“
SPG	Sicherheitspolizeigesetz BGBl 1991/566
StGB	Strafgesetzbuch BGBl 1974/60
StGG	Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger RGBI 1867/142
StMV	Standard- und Muster-Verordnung 2000 BGBl II 2000/201
StPO	Strafprozessordnung 1975 BGBl 631 (Wv)
StProt	stenographische(s) Protokoll(e)
SZ	„Entscheidungen des österreichischen Obersten Gerichtshofes in Zivil- (und Justizverwaltungs-)sachen“
ua	unter anderem
uä	und ähnliche(s)
uU	unter Umständen

va	vor allem
VersVG	Versicherungsvertragsgesetz 1958 BGBl 1959/2
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
vgl	vergleiche
VwGH	Verwaltungsgerichtshof
wbl	„wirtschaftsrechtliche Blätter“
WLAN	Wireless Local Area Network
Wv	Wiederverlautbarung
Z	Zahl, Ziffer
zB	zum Beispiel
ZfV	„Zeitschrift für Verwaltung“
ZfVBDat	Ausgewählte Beschlüsse der Datenschutzkommission und des Datenschutzrates in chronologischer Folge
ZPO	Zivilprozeßordnung RGBI 1895/113

1. Einführung

1.1 Einleitung

In den letzten Jahren hat die Technik in unserem Leben enorm an Bedeutung gewonnen: Das Telefonieren mit einem Mobiltelefon, das eine Ortung des Gesprächsteilnehmers ermöglicht, das Bezahlen mit Kreditkarte oder das Surfen im Internet sind selbstverständlich geworden. Oft ist man sich dabei aber nicht bewusst, dass beispielsweise der Mobilfunknetz-Betreiber mitverfolgen kann, wo man sich aufgehalten hat, dass bei der Zahlung per Kreditkarte ein Profil über die Kaufgewohnheiten erstellt wird und dass der Provider genau nachverfolgen kann, welche Seiten man im Internet besucht hat. Dem Datenschutz kommt im Zeitalter der weltweiten Wissens- und Informationsgesellschaft eine immer größere Bedeutung zu: Computersysteme werden weltweit vernetzt und die Entwicklung neuer Techniken schreitet rasch voran. Was heute noch die Ausnahme darstellt, kann morgen bereits zur Regel geworden sein. So wird seit kurzem in Londons Innenstadt jedes einzelne Kfz-Kennzeichen von hunderten Videokameras registriert und mit einer zentralen Datenbank verglichen, um eine Maut verrechnen zu können. Die europäische Kommission überlegt, den USA vollen Zugriff auf die Flugbuchungssysteme europäischer Fluglinien zu gewähren (mit allen erfassten Daten wie etwa ob ein Passagier ein fleischloses Menü gewünscht hat oder ob er einen Nichtraucher-Platz wollte). Jeder einzelne Österreicher ist von Geburt an bis zu seinem Tod (und darüber hinaus) in beinahe hundert Datenbanken (vom Schulregister über das Melderegister bis hin zu diversen Datenbanken privater Unternehmen wie etwa Versicherungen oder Banken) gespeichert. Sowohl öffentliche als auch private Organisationen sammeln akribisch sämtliche verfügbaren Daten, und die Zahl dieser Sammler von personenbezogenen Daten wird in Zukunft noch steigen. Durch die Möglichkeit der Verknüpfung mehrerer Datenbanken erscheint die Orwell'sche Schreckensvision des allwissenden „großen Bruders“ nicht mehr völlig undenkbar und deswegen wurde schon vor mehr als zwei Jahrzehnten der Datenschutz in Österreich gesetzlich verankert.

Doch was nun, wenn der Datenschutz und damit die Privatsphäre erwiesenermaßen verletzt wurden und der Betroffene dadurch einen Schaden erlitten hat? Reicht es bloß die Rechtsverletzung (wenn auch gerichtlich)

festzustellen oder soll dem Geschädigten darüber hinaus auch noch eine weitere Sanktionsmöglichkeit gegeben werden? Der (europäische) Gesetzgeber hat sich für die zweite Möglichkeit entschieden: Bei Verletzung des Datengeheimnisses soll dem Betroffenen in Gestalt von § 33 DSG 2000 die Möglichkeit zur Geltendmachung von Schadenersatzansprüchen gegeben werden. Dabei wird in Österreich nicht nur der entstandene materielle Schaden ersetzt, sondern unter gewissen Umständen auch der durch die öffentliche Bloßstellung erlittene immaterielle Schaden; außerdem kommen dem Betroffenen mehrere Erleichterungen zugute, falls er eine Schadenersatzklage erhebt.

Das erste Kapitel dieser Arbeit widmet sich der Frage, was Datenschutz überhaupt bedeutet und liefert eine kurze Übersicht über die historische Entwicklung des Datenschutzes in Österreich sowie über die Rechtslage betreffend Schadenersatzansprüche aus Datenschutzverletzungen vor Inkrafttreten des DSG 2000. Im zweiten Kapitel wird auf das Grundrecht auf Datenschutz und auf die verfassungsrechtliche Komponente des Datenschutzes eingegangen und im dritten Kapitel wird ein kurzer Überblick über das DSG 2000 mitsamt seinen Begriffsdefinitionen gegeben und dargestellt, wie das Datengeheimnis geschützt wird. Das vierte Kapitel bildet den Hauptteil dieser Arbeit und widmet sich dem Thema „Schadenersatz nach § 33 DSG 2000“. Dabei wird zuerst geklärt, wann es überhaupt zur Anwendung des § 33 kommen kann: Nämlich grundsätzlich nur in jenen Fällen, in denen der Auftraggeber (und somit der Beklagte) nicht dem öffentlichen (behördlichen) Bereich zuzurechnen ist. Danach werden anhand der allgemeinen Voraussetzungen für den Ersatz von Schäden die Besonderheiten herausgearbeitet, auf die es bei der Geltendmachung von Schadenersatzansprüchen ankommt, die ihre Wurzel im DSG 2000 haben. Auch wird die Frage der Ersatzfähigkeit immaterieller Schäden und die prozessuale Seite behandelt werden. Im fünften Kapitel wird § 33 weiters kritisch hinterfragt und ua erörtert, ob die DS-RL korrekt ins österreichische Recht transformiert worden ist. Das sechste Kapitel liefert schließlich eine Übersicht über den „Gegenpol“ dieser Arbeit, nämlich die Geltendmachung von Schadenersatzansprüchen aus Datenschutzverletzungen gegenüber Auftraggebern des öffentlichen Bereichs.

1.2 Was bedeutet Datenschutz?

Mit dem Sammeln von Daten durch den Staat wurde schon lange vor dem Computer-Zeitalter begonnen¹ und im beginnenden 21. Jahrhundert nimmt die Intensität der Nutzung von Computern (sowohl in der Form von Einzelplatzrechnern wie etwa handelsüblichen PCs als auch in Gestalt von Großrechnern) in allen Bereichen des öffentlichen und privaten Lebens ständig zu. An Arbeitsplätzen finden sich PCs, welche oft mit anderen Rechnern im Firmennetzwerk verbunden sind und durch den Boom des World Wide Web in den letzten Jahren sind diese Computer nicht selten noch zusätzlich mit dem weltweit größten Computernetzwerk, dem Internet, verbunden. Dabei werden immer mehr Daten über den Benutzer gesammelt, gespeichert und archiviert. Auf der einen Seite kommt es dadurch zu einer Steigerung der Effizienz der Verwaltung, auf der anderen Seite kommt es durch unmittelbaren Zugriff und Verknüpfung von verschiedenen Datenbeständen zu einer immer weiter fortschreitenden Einschränkung der Privatsphäre des Einzelnen. *„Information ist eine wesentliche Komponente der Machtentfaltung und birgt daher auch die Gefahr eines Machtmissbrauches in sich.“*²

Man (bewusst nicht „der Staat“ – siehe Kapitel 2.1 über die Drittwirkung des Grundrechts auf Datenschutz) soll nicht uneingeschränkt und völlig frei über personenbezogene Daten verfügen können, sondern es gilt einen Interessensausgleich herzustellen: Einerseits soll das Recht auf informelle Selbstbestimmung verhindern, dass der Einzelne von Staat und Wirtschaft abhängig wird, weil diese Stellen immer mehr von ihm wissen, andererseits könnten insbes staatliche Einrichtungen oft nicht effizient genug agieren, wenn sie ausschließlich auf die freiwillige Mitwirkung der Bürger angewiesen wären.³

„Datenschutz“ bedeutet, dass bei Datenverarbeitung bzw –erarbeitung diese Daten den datenschutzrechtlichen Vorschriften entsprechend behandelt werden sollten - *„Nicht der gläserne Mensch, sondern der gläserne Computer ist Ziel des Datenschutzes.“*⁴

¹ *Jahnel*, Datenschutzrecht, in *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht² (2003) 241 (243).

² *Adamovich/Funk*, Allgemeines Verwaltungsrecht³ (1987) 310.

³ *Koitz*, Informatikrecht schnell erfasst (2002) 233.

⁴ *Tinnefeld/Tubies*, Datenschutzrecht² (1989) 8.

1.3 Die Geschichte des Datenschutzes in Österreich

Bereits 1967 wurde von einer Datenverarbeitungsanlage zu Planungszwecken für das Bundesheer ausgegangen⁵, jedoch fand die Frage des Datenschutzes bis zum Beginn der Siebziger-Jahre des vorigen Jahrhunderts kaum Beachtung in der rechtswissenschaftlichen Diskussion, obwohl bereits die Regierungserklärung 1971 auf ein zu schaffendes Datenschutzgesetz Bezug nahm. Während der Siebziger-Jahre wurde (ausgehend von der Diskussion in den USA) die zunehmende Speicherung und Verwendung von personenbezogenen Daten jedoch immer mehr hinterfragt und die Forderung nach Datenschutz wurde immer lauter. In den letzten 30 Jahren hat die rechtswissenschaftliche Diskussion um den Datenschutz schließlich eine umfassende Erweiterung erfahren.

Die Entwicklung von Datenschutznormen kann in vier Generationen eingeteilt werden:

Die erste Generation des Datenschutzes:

Die erste Generation von Datenschutznormen richtete sich gegen zentrale nationale Datenbanken, die sowohl vom Staat als auch von Unternehmen zur Zentralisierung der Datenverarbeitung angelegt werden hätten sollen. Die computerunterstützte Datenverarbeitung wurde als technisches „Großrisiko“ ähnlich der Kernenergie gesehen und sollte verhindert werden⁶, indem eine Konzentration auf wenige Großdatenbanken durch den Staat überwacht werden sollte. Zu den Datenschutznormen der ersten Generation zählen ua das Hessische Datenschutzgesetz 1970, das schwedische Datenschutzgesetz 1973 oder die RV zum österreichischen Datenschutzgesetz 1974⁷, welches jedoch nicht vom Nationalrat verabschiedet wurde.

Die zweite Generation des Datenschutzes:

Die technologische Entwicklung verlief jedoch nicht wie erwartet: Die Computertechnologie entwickelte sich nicht in die Richtung von wenigen zentralen Großcomputern, sondern der Trend ging zu immer kleineren, leistungsfähigeren

⁵ Reimann, Der Datenschutz in Österreich – vom Datenschutzgesetz 1978 bis zum Datenschutzgesetz 2000 (2001) 12.

⁶ Mayer-Schönberger/Brandl, Datenschutzgesetz 2000 (1999) 13.

⁷ ErläutRV 72 BlgNR 14. GP.

und günstigeren Kleincomputern wie zB den Apple II, der den Siegeszug des PCs ebnete und somit wurden letztendlich die Pläne zur Schaffung von zentralen Datenbanken nicht verwirklicht. Mit dieser neuen technologischen Entwicklung änderte sich auch das Gefährdungspotential: Datenschutzrechtliche Normen mussten nicht mehr nur auf einige wenige zentrale Datenbanken, sondern auch auf unzählige EDV-Anlagen in Verwaltung und Wirtschaft angewendet werden. Immer mehr Bürger nahmen die mögliche Gefährdung durch die Verarbeitung ihrer personenbezogenen Daten wahr oder wurden von den Medien darüber informiert, wodurch der Begriff der datenschutzrechtlichen Betroffenenrechte immer bedeutender wurde und schließlich auch von den Bürgern eingefordert wurde. In Datenschutznormen der zweiten Generation finden sich verstärkt Betroffenenrechte, die nachhaltige Abschwächung der technikgestaltenden Normen früherer Datenschutzansätze sowie die Betonung des Schutzes der Privatsphäre. Zu dieser zweiten Generation von Datenschutznormen gehört auch das österreichische DSG 1978⁸, das am 18.10.1978 vom Nationalrat verabschiedet wurde und am 1.1.1980 in Kraft trat.

Die Vorbereitungen zum DSG 1978 waren äußerst intensiv und umfangreich, es bedurfte 3 Jahre intensivster Vorbereitung auf Regierungsebene und einer 4-jährigen ebenfalls sehr intensiven Vorbereitungszeit auf parlamentarischer Ebene. Österreich war mit der Erlassung des DSG 1978 der neunte Staat weltweit, der den Datenschutz gesetzlich verankert hatte (das erste Land, das über ein Datenschutzgesetz verfügte war Schweden, welches 1973 ein entsprechendes Gesetz erließ, es folgten ua 1974 die USA mit dem so genannten Privacy-Act, 1976 die Bundesrepublik Deutschland mit dem Bundesdatenschutzgesetz sowie Datenschutzgesetze in Ländern wie Kanada, Neuseeland, Dänemark und Norwegen). Österreich war insoweit weltweit in der Vorreiterrolle, als das DSG 1978 erstmals eine verfassungsrechtliche Verankerung des Datenschutzes als Grundrecht enthielt.

Der zentrale Inhalt dieses Gesetzes war (naturgemäß) der Schutz personenbezogener Daten. Grundsätzlich wurden sowohl die öffentliche Verwaltung als auch Private zur Geheimhaltung personenbezogener Daten

⁸ BG vom 18.10.1978 über den Schutz personenbezogener Daten (Datenschutzgesetz-DSG) BGBl 1978/565.

verpflichtet, ebenso durften nur solche Daten verarbeitet werden, bei denen ein Zusammenhang mit dem rechtlich anerkannten Unternehmensgegenstand bzw der Zuständigkeit der Behörde gegeben war. Schon nach dem DSG 1978 war für die Weitergabe von Daten eine Rechtsgrundlage erforderlich und eine Weitergabe von schutzwürdigen Daten grundsätzlich untersagt. Vom Recht auf Geheimhaltung waren sowohl automationsunterstützte als auch nicht automationsunterstützte (konventionelle) Daten erfasst, die Rechte auf Auskunft, Richtigstellung und Löschung bezogen sich jedoch nur auf automationsunterstützt verarbeitete Daten. Ebenfalls im DSG 1978 enthalten waren Strafbestimmungen bei Verletzungen des Datenschutzgesetzes, die berufliche Pflicht zur Verschwiegenheit sowie Anordnungen zu Datensicherungsmaßnahmen.

Die dritte Generation des Datenschutzes:

Der Datenschutz entwickelte sich zwar zu einem Abwehrrecht, wurde von den Bürgern jedoch kaum in Anspruch genommen, da es dem Einzelnen kaum möglich ist, die Informationsbedürfnisse anderer abzuwehren, ohne dabei selbst isoliert zu werden. Unterstützt durch das Wiederaufleben partizipativer Ideen in den Achtziger- Jahren wurde der Datenschutz in der dritten Generation als Gestaltungsrecht konzipiert – der Einzelne sollte die Möglichkeit zur Mitbestimmung und –gestaltung bei der Verwendung seiner personenbezogenen Daten bekommen. Zum Leitgedanken in der Entwicklung des europäischen Datenschutzes wurde das Grundrecht auf informationelle Selbstbestimmung, das zum ersten Mal im „Volkszählungsurteil“⁹ des deutschen Bundesverfassungsgerichts aus dem Jahr 1983 angesprochen wurde: Nach dem deutschen Volkszählungsgesetz 1983 sollte eine Volks- und Berufszählung durchgeführt werden. Gegen dieses Gesetz erfolgte eine Beschwerde beim Bundesverfassungsgericht, welches feststellte, dass die erhobenen Daten für andere als statistische Zwecke nicht zur Verfügung stehen würden und daher auch nicht mit den Daten anderer Stellen abgeglichen werden dürften. Das Erstellen eines lückenlosen Persönlichkeitsbildes des einzelnen Bürgers durch die Zusammenführung von Volkszählungsdaten wurde als unzulässig erachtet, Einschränkungen des Rechts auf „informationelle Selbstbestimmung“ seien nur im überwiegenden Allgemeininteresse zulässig. Dieses neue Grundrecht wurde zum

⁹ BVerfG 15.12.1983, BVerfGE 65, 1 = EuGRZ 1983, 577 = NJW 1984, 419.

Ausgangspunkt jeglichen Datenschutzes gemacht, gleichzeitig zeigte das Gericht aber auch auf, dass die Einschränkung der Herrschaft des Einzelnen über seine Daten jedoch im Allgemeininteresse zulässig sei.

Die vierte Generation des Datenschutzes:

Auch die informationelle Selbstbestimmung gab den Bürgern nicht ausreichend Möglichkeit zur Geltendmachung ihrer Rechte, weil es beispielsweise während Vertragsverhandlungen oft routinemäßig zum Verzicht auf Datenschutzrechte kam. Zudem entstanden neue Problembereiche (wie zB im Direktmarketingbereich oder in der Telekommunikation), durch die sich bisher geltende Datenschutznormen als unzureichend erwiesen. Datenschutzbestimmungen der vierten Generation schützen besonders Betroffenenrechte. Es ist zu einer Erweiterung der Haftung durch Verschuldensregelungen und Beweislastumkehr gekommen, auch trat auch noch eine Haftungsergänzung durch sektorale Vorschriften hinzu (zB durch die Telekommunikationsrichtlinie¹⁰). Im Jahr 1995 erließ die EU die Datenschutzrichtlinie:¹¹ Ziel der Richtlinie war ein möglichst ungehinderter Datenfluss personenbezogener Daten innerhalb der Europäischen Union, der Schutz wurde auf manuelle Verarbeitungen erweitert und auf alle Verarbeitungsschritte ausgedehnt. Dadurch wurde Österreich zu einer tief greifenden Erneuerung des Datenschutzrechts verpflichtet. Als Konsequenz wurde das DSG 2000¹² am 13.7.1999 vom NR verabschiedet und trat am 1.1.2000 in Kraft, wobei die bisherige Trennung des einfachgesetzlichen Teils des DSG 1978 in einen privaten und einen öffentlichen Teil aufgegeben wurde. Damit hat die Entwicklung des Datenschutzes in Österreich ihre vorerst letzte Stufe erreicht.

¹⁰ Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ABIL 024, 1 vom 30.1.1998.

¹¹ 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 (EG-Datenschutzrichtlinie), ABIL 281, 31 vom 13.11.1995.

¹² BG vom 17.8.1999 über den Schutz personenbezogener Daten (Datenschutzgesetz 2000-DSG) BGBl I 1999/165.

1.4 Exkurs: Schadenersatz im DSG 1978

Im DSG 1978 wurde die Frage des Schadenersatzes nach einer Verletzung des Datengeheimnisses im privaten Bereich nicht ausdrücklich geregelt: § 28 Abs 1 DSG 1978 verwies unter dem Titel „zivilrechtliche Haftung“ für Fälle von Verletzungen des Datengeheimnisses den Betroffenen auf den ordentlichen Rechtsweg, die DSK war schon nach dem DSG 1978 nicht für die Geltendmachung von Schadenersatzansprüchen bei Verletzungen des Datenschutzgesetzes im privaten Bereich zuständig. Wurden Daten entgegen den Bestimmungen des DSG 1978 oder den aufgrund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen verarbeitet, benützt oder übermittelt, so stellte Abs 2 klar, dass der Betroffene, unbeschadet etwaiger Ansprüche auf Schadenersatz, Anspruch auf Unterlassung und Beseitigung des dem DSG bzw den aufgrund des DSG erlassenen Durchführungsbestimmungen widerstreitenden Zustandes hatte. Hinsichtlich der Geltendmachung von Schadenersatzansprüchen aufgrund von Verletzungen von datenschutzrechtlichen Bestimmungen wurde der Betroffene auf die allgemeinen Schadenersatzregelungen des ABGB in Gestalt der §§ 1293ff verwiesen; eine dezidierte Regelung der Schadenersatzansprüche wurde offen gelassen. Der Grund dafür lag darin, dass sich ansonsten die Erlassung des DSG 1978 noch mehr verzögert hätte.¹³ Gleichzeitig mit der Verabschiedung des DSG 1978 kam es zu einer EntschlieÙung des NR¹⁴, die Bundesregierung möge ehestmöglich eine Regierungsvorlage über ein Bundesgesetz vorlegen, durch das die zur Ergänzung des DSG 1978 nötigen schadenersatzrechtlichen Bestimmungen eingefügt werden sollten. Insbesondere sollten die Möglichkeiten einer Vereinfachung der Haftung, einer eingeschränkten Erfolgshaftung sowie eines Ersatzes immaterieller Schäden für den Bereich des Datenschutzes geprüft werden. Der Gesetzgeber konnte sich jedoch bis zur Erlassung des DSG 2000 nicht dazu durchringen, dieser EntschlieÙung des NR nachzukommen und erst (bedingt durch die DS-RL) im DSG 2000 finden sich in Gestalt des § 33 schadenersatzrechtliche Regelungen hinsichtlich einer Beweislastumkehr zugunsten des Betroffenen (Abs 3) und hinsichtlich des Ersatzes immaterieller Schäden (Abs 1 iVm § 7 MedG).

¹³ StProt NR 104. Sess 14. GP 10229.

2. Grundsätze des Datenschutzes

2.1 Das Grundrecht auf Datenschutz

Beim Datenschutz handelt es sich um ein besonderes Mittel des Schutzes der Privatheit.¹⁵ Das Grundrecht auf Datenschutz wird durch die Verfassungsbestimmung des § 1 DSG 2000 normiert und in den einfachgesetzlichen Bestimmungen der §§ 4 bis 64 näher ausgeführt. Jedermann wird ein Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gewährt, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen dieses Interesses wird verneint, wenn Daten einem Geheimhaltungsanspruch nicht zugänglich sind, weil sie allgemein verfügbar oder nicht auf den Betroffenen rückführbar sind.¹⁶ Durch die Formulierung des § 1 („jedermann“) kommt zum Ausdruck, dass es sich dabei um ein Jedermannsrecht handelt, das allen Menschen (unabhängig von deren Staatsbürgerschaft) zusteht und auch von juristischen Personen beansprucht werden kann (die DS-RL sieht im Gegensatz dazu keine Ausdehnung des Grundrechtes auf juristische Personen vor, sondern richtet sich ausschließlich an natürliche Personen, vgl Art 1 Abs 1 DS-RL sowie Erwägungsgrund 24). Es handelt sich um kein einheitliches Grundrecht auf Datenschutz, vielmehr besteht dieses aus mehreren, unterschiedlichen Rechten.¹⁷ Diese sind:

1. das Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1),
2. das Recht auf Auskunft (§ 1 Abs 3 Z 1),
3. das Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2),
4. das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs 3 Z 2).

Beschränkungen des Grundrechtes auf Datenschutz sind nach § 1 Abs 2 DSG 2000 zulässig, wenn einerseits die Verwendung von personenbezogenen Daten im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt oder aber andererseits „zur Wahrung überwiegender berechtigter Interessen eines anderen“ nötig ist. Das Vorliegen letzterer Voraussetzung ist vom Gesetzgeber,

¹⁴ JAB 1024 BlgNR 14. GP 22.

¹⁵ *Ermacora*, Grundriß der Menschenrechte in Österreich (1988) Rz 601.

¹⁶ *Walter/Mayer*, Grundriß des österreichischen Bundesverfassungsrechts⁹ (2000) Rz 1489.

¹⁷ *Jahnel in Jahnel/Schramm/Staudegger*, Informatikrecht², 250.

aber auch von den jeweils zur Vollziehung des § 1 verpflichteten Organen im Zuge verfassungskonformer Interpretation zu beurteilen.¹⁸

Anders als bei konventionellen Grundrechten normiert die Verfassungsbestimmung des § 1 Abs 5 eine ausdrückliche unmittelbare Drittwirkung des Grundrechts: *„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.“* Der Begriff „Rechtsträger“ umfasst juristische Personen des öffentlichen und privaten Rechts sowie natürliche Personen¹⁹ - das Grundrecht auf Datenschutz wirkt somit nicht nur zwischen dem Einzelnen und dem Staat, sondern auch im Privatrechtsverkehr zwischen den Bürgern untereinander.

Eingriffe einer staatlichen Behörde sind nur aufgrund von Gesetzen zulässig und stehen unter dem materiellen Gesetzesvorbehalt des Art 8 Abs 2 MRK. Demzufolge sind Eingriffe nur erlaubt, wenn sie in einer demokratischen Gesellschaft zB zum Schutz der nationalen Sicherheit, der öffentlichen Ruhe und Ordnung oder der Rechte und Freiheiten anderer notwendig sind. Zudem müssen Eingriffe auf das Erforderliche beschränkt bleiben²⁰ und jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.²¹ Mit anderen Worten: Ein Eingriff in das Grundrecht auf Datenschutz ist zulässig, wenn eine zur Datenerhebung ermächtigende Norm den Informationseingriff gestattet, dieser einem der enumerativ aufgezählten Eingriffsziele dient sowie auf das Erforderliche beschränkt ist und einem demokratischen Staat angemessen ist.²²

Im privaten Bereich ist für die Beurteilung der Zulässigkeit eines Eingriffs in das Grundrecht auf Datenschutz eine Interessensabwägung zwischen dem Eingreifenden und dem Betroffenen im Einzelfall durchzuführen²³ und die

¹⁸ *Walter/Mayer*, Grundriß⁹ Rz 1491.

¹⁹ VfGH 12.10.1989, VfSlg 12.194/1989.

²⁰ *Öhlinger*, Verfassungsrecht⁵ (2003) Rz 830.

²¹ *Walter/Mayer*, Grundriß⁹ Rz 1491; *Souhrada-Kirchmayr*, Das Datenschutzgesetz 2000, SozSi 2000, 938 (941).

²² VfGH 30.11.1989, VfSlg 12.228/1989.

²³ *Jahnel* in *Jahnel/Schramm/Staudegger*, Informatikrecht², 251.

einfachgesetzlichen Ausführungsbestimmungen der §§ 7 bis 9 sind heranzuziehen.

Voraussetzung für das Bestehen eines Grundrechts auf Datenschutz ist, dass überhaupt personenbezogene Daten (§ 4 Z 1) vorliegen, die auf eine in ihrer Identität bestimmbare Person zurückgeführt werden können und weiters, dass diese Daten überhaupt geheim gehalten werden können und sie also nicht frei zugänglich sind. Wichtig dabei ist die faktische Unmöglichkeit der Geheimhaltung.²⁴ Eine Verwendung von zulässigerweise veröffentlichten Daten (§§ 8 Abs 2, 12 Abs 3 Z 1, 17 Abs 2 Z 1) schließt ein schutzwürdiges Geheimhaltungsinteresse jedenfalls aus. Dadurch soll die Verwendung von Daten, die öffentlich zugänglich sind, ermöglicht werden, ohne jedoch einen Missbrauch (in der Gestalt von zweckfremder Verwendung) zu ermöglichen. Die Verpflichtung zur Geheimhaltung schutzwürdiger personenbezogener Daten besteht weiters unabhängig von der Form der Verarbeitung dieser Daten und betrifft somit auch manuelle Daten, sofern diese zur Verarbeitung in manuellen Dateien bestimmt sind (wie zB Karteikarten, Akten oder Notizzettel).

Beim Grundrecht auf Datenschutz handelt es sich um ein höchstpersönliches Recht – es steht nur lebenden Personen zu. Allerdings ist zu beachten, dass Daten Verstorbener gleichzeitig auch auf Lebende Bezug nehmen können und deswegen unter Umständen als personenbezogene Daten dieser (lebenden) Personen zu qualifizieren sind.

Zur Durchsetzung des Anspruchs auf Geheimhaltung sowie zur Ahndung einer erfolgten Verletzung ist gem § 1 Abs 5 iVm § 32 Abs 1 im privaten Bereich grundsätzlich die ordentliche Gerichtsbarkeit und im öffentlichen Bereich die DSK zuständig. Damit wurde die durch das DSG 1978 erfolgte traditionelle Teilung des Rechtsschutzes in einen privaten und einen öffentlichen Bereich aufrechterhalten. Entscheidend ist nicht der Inhalt der Tätigkeit, sondern die rechtliche Organisationsform des Auftraggebers, wobei eine Tätigkeit trotz der Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze - zB durch Beleihung oder Ausgliederung – und somit die Privatwirtschaftsverwaltung dem öffentlichen

²⁴ Souhrada-Kirchmayr, SozSi 2000, 941.

Bereich (§ 5 Abs 2) zugerechnet wird. Das Recht auf Auskunft ist jedoch gem § 1 Abs 5 ausnahmslos und unabhängig von der Organisationsform des Auftraggebers bei der DSK durchsetzbar.

2.2 Datenschutz und Verfassung

Die Verfassungsbestimmung des § 2 DSG 2000 ist die vorrangige Kompetenzgrundlage für Gesetzgebung und Vollziehung in Datenschutzangelegenheiten. Demnach ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr Bundessache. Die Vollziehung solcher Bundesgesetze steht gem Abs 2 ebenfalls dem Bund zu. Werden jedoch automationsunterstützte Daten von einem Land, im Auftrag eines Landes oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet, so ist die Vollziehung Ländersache, soweit nicht durch Bundesgesetz die DSK, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Hinsichtlich der Gesetzgebungskompetenz bei manuellen Datenverarbeitungen konnte keine Einigung mit den Ländern erzielt werden²⁵, es besteht somit keine generelle Kompetenz des Bundes. Die Zuständigkeit richtet sich danach, ob die Angelegenheiten bezüglich der Dateien in die Kompetenz des Bundes oder gem Art 15 B-VG in die der Länder fällt. In letzterem Fall ist es Aufgabe der Länder, Datenschutzbestimmungen auf Länderebene zu erlassen und somit die DS-RL umzusetzen.²⁶

²⁵ *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz-Regierungsvorlage, *ecolex* 1999, 361 (362).

²⁶ Vgl das Steiermärkische Datenschutzgesetz (StDSG), LGBISt 2001/39.

3. Überblick über das DSG 2000

Wie bereits im vorigen Kapitel erwähnt ist das DSG 2000 so konzipiert, dass durch die Verfassungsbestimmung des § 1 ein Grundrecht auf Datenschutz gewährt wird: Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, soweit ein schutzwürdiges Interesse daran besteht. Um die Frage beantworten zu können, was vom Datengeheimnis iSd DSG 2000 umfasst wird, stellt sich zuerst die Frage, was überhaupt datenschutzrechtlich „personenbezogene Daten“ sind, wer den Schutz seiner Daten in Anspruch nehmen kann, gegen wen sich dieser Schutz richtet und wie das DSG 2000 systematisch aufgebaut ist.

3.1 Definitionen

3.1.1 Personenbezogene Daten

Wie viele andere datenschutzrechtliche Definitionen werden auch die Begriffe „Daten“ bzw „personenbezogene Daten“ in § 4 definiert: § 4 Z 1 setzt beide Begriffe gleich und beschreibt sie als Angaben über Betroffene (iSd § 4 Z 3), deren Identität bestimmt oder bestimmbar ist. Durch die DS-RL musste die bisherige Einschränkung der Definition nach DSG 1978 „auf einem Datenträger festgehalten“ entfallen und auch die bisherige Einschränkung der Bestimmbarkeit „mit hoher Wahrscheinlichkeit“ wurde verworfen, da sie sich in der Praxis als wenig bedeutsam erwiesen hat.²⁷ Somit fordert das DSG 2000 nunmehr nicht mehr eine nur auf hoher Wahrscheinlichkeit basierende Bestimmbarkeit, sondern Identifizierbarkeit auf sicherer Basis. Auch müssen die betreffenden Daten geheim gehalten werden können, was grundsätzlich unmöglich ist, wenn es sich um allgemein zugängliche Daten (wie etwa Telefonbücher) handelt, wobei die allgemeine Verfügbarkeit nicht mit einer Veröffentlichung an sich gleichzusetzen ist.²⁸ Beispiele für personenbezogene Daten iSd DSG 2000 sind etwa der Name, das Geburtsdatum, das Religionsbekenntnis, die Adresse, Angaben über das Vermögen, Informationen über individuelle Kenntnisse und Fähigkeiten einer Person, aber auch Werturteile²⁹ (wie zB die Aussage „XY ist ein schlechter Zahler“

²⁷ ErläutRV 1613 BlgNR 20. GP 36f.

²⁸ Souhrada-Kirchmayr, SozSi 2000, 940f.

²⁹ Dohr/Pollirer/Weiss, Datenschutzrecht² (2002) 46.

bezogen auf die Bonität). Der VfGH hat in seinem Erkenntnis³⁰ aus dem Jahr 1989 festgestellt, dass auch Wirtschaftsdaten, die in Folge von statistischen Erhebungen ermittelt werden, datenschutzrechtlich als personenbezogene Daten gelten. Aufgrund der Angaben muss die Bestimmbarkeit des Betroffenen beim Verwender oder bei einem Dritten (vom Betroffenen Verschiedenen, zB der Inhaber des Entschlüsselungscodes bei codierten Daten) vorliegen. Daher ermöglichen auch Reisepassnummern oder Kfz-Kennzeichen eine derartige Bestimmbarkeit und sind daher als (allerdings nur indirekt) personenbezogene Daten anzusehen. Werden mehrere Merkmale, die jeweils isoliert betrachtet keinen Personenbezug aufweisen, miteinander kombiniert und verknüpft, so kann dadurch ebenfalls eine Bestimmbarkeit erzeugt werden (zB durch Verknüpfung von Alter, Zahl der Kinder und Arbeitsort).³¹ Auf die Art der Datenspeicherung (zB auf CD-ROM, Festplatte, Papier, Mikrofilm uä) kommt es jedenfalls nicht an.

Anders als Art 1 Abs 1 DS-RL bezieht die Daten-Definition des DSG 2000 nicht nur Angaben über natürliche Personen, sondern auch Informationen über juristische Personen und Personengemeinschaften ein und geht somit weiter als die DS-RL. Vom Begriff nicht erfasst sind jedoch auch weiterhin (analog zur DS-RL) Daten über Verstorbene oder rechtlich nicht mehr existente juristische Personen oder Personengemeinschaften.

3.1.1.1 Nur indirekt personenbezogene Daten

Schon die DS-RL unterscheidet zwischen direkter und nur indirekter Identifizierbarkeit von Betroffenen. Der österreichische Gesetzgeber hat diese Idee aufgegriffen und in § 4 Z 1 definiert, wann Daten „nur indirekt personenbezogen“ sind: Es handelt sich dabei um Fälle, in denen es für den konkreten Verwender der Daten nicht möglich ist den (zB in Form einer fortlaufenden Nummer) vorhandenen Personenbezug auf eine in ihrer Identität bestimmbare Person zurückzuführen. Für die Beurteilung der Frage, ob der Verwender die Identität des Betroffenen bestimmen kann, wird durch § 4 Z 1 letzter Satz ausschließlich auf die Verwendung legaler Mittel durch den Verwender abgezielt. Bei richtlinienkonformer Interpretation werden jedoch zusätzlich auch

³⁰ VfGH 30.11.1989, VfSlg 12.228/1989.

³¹ *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 117f.

noch „mögliche“ Mittel zu berücksichtigen sein.³² Weiters ist noch zu beachten, dass nach Erwägungsgrund 26 der RL nur diejenigen Mittel der Identifikation als solche anzusehen sind, die „vernünftigerweise“ angewendet werden und somit nicht vollkommen ungewöhnlich sind. Zwar sind diese Daten grundsätzlich rückführbar (und damit personenbezogen), jedoch nur für denjenigen, der den Schlüssel dafür rechtmäßig besitzt oder ihn sich gleichermaßen beschafft. Der Gebrauch solcher nur indirekt personenbezogenen Daten ist dann im konkreten Fall für diesen einzelnen Verwender unter erleichterten Bedingungen erlaubt und zulässig. Für diese Datenart wird die Verwendung von Daten im Inland durch §§ 8 Abs 2 und 9 Z 2 vereinfacht und die Übermittlung und Überlassung ins Ausland genehmigungsfrei gestattet (§ 12 Abs 3 Z 2). Außerdem werden Datenanwendungen als nicht meldepflichtig erklärt (§ 17 Abs 2 Z 3), es werden die Rechte der §§ 26 bis 28 (Auskunftsrecht, Recht auf Richtigstellung oder Löschung, Widerspruchsrecht) für Betroffene eingeschränkt (§ 29) und es gelten spezielle Regelungen bezüglich wissenschaftlicher Forschung und Statistik mit solchen Daten (§ 46 Abs 1 Z 3 und Abs 5). Beispiele für nur indirekt personenbezogene Daten sind etwa Sozialversicherungsnummern oder Kfz-Kennzeichen.

3.1.1.2 Anonymisierte Daten

Sowohl von den personenbezogenen als auch von den nur indirekt personenbezogenen Daten sind diejenigen Daten zu unterscheiden, die üblicherweise als „anonymisierte Daten“ bezeichnet werden. Es handelt sich dabei um Daten, bei denen kein Personenbezug vorliegt, weil dieser nicht mehr herstellbar ist und niemand durch diese Daten auf eine individuell bestimmbare Person rückschließen kann. Folglich ist diese Datenart auch nicht datenschutzrechtlich relevant. In Betracht kommen etwa die Ergebnisse einer anonym durchgeführten Umfrage, bei der zwar an sich personenbezogene Daten wie Familienstand, Zahl der Kinder oder Blutgruppe abgefragt wurden, aufgrund der völligen Anonymität der Fragebögen jedoch kein Personenbezug möglich ist.

³² Ghali, Datenschutz Rechtsgrundlagen (1999) 140.

3.1.1.3 Sensible Daten

In Umsetzung des Art 8 Abs 1 DS-RL enthält das DSG 2000 nun in § 4 Z 2 die Kategorie der „sensiblen Daten“, bei denen die Gefahr einer diskriminierenden Verwendung besonders hoch ist. Es handelt sich dabei um eine taxative Aufzählung, die Daten natürlicher Personen über ihre rassische und ethnische Herkunft, ihre politische Meinung, ihre Angehörigkeit zu Gewerkschaften, ihre religiöse oder philosophische Überzeugung, ihre Gesundheit oder ihr Sexualleben miteinschließt. Es kommt nicht darauf an, ob im konkreten Fall ein Diskriminierungsrisiko nahe liegt, sondern bereits die Einordnung in eine der Datenkategorien ist entscheidend. Ebenso unbeachtlich ist die Frage, ob die Daten unmittelbar oder nur mittelbar einen sensiblen Informationsgehalt darstellen.³³ Die Verwendung von Gesundheitsdaten durch private Versicherungsnehmer unterliegt jedenfalls dem DSG 2000 und die Versicherer dürfen personenbezogene Gesundheitsdaten nur in gesetzlich vorgegebenen Fällen verwenden.³⁴

3.1.2 Betroffener

Betroffener ist gem § 4 Z 3 jede vom Auftraggeber verschiedene (auch ausländische) natürliche oder auch juristische Person oder Personengemeinschaft, deren Daten iSd § 4 Z 8 verwendet werden. Als Personengemeinschaft gilt sowohl eine handelsrechtliche Personengesellschaft (wie zB eine OHG gem §§ 105ff HGB oder eine KG gem §§ 161ff HGB) als auch eine sonstige Personengemeinschaft ohne Rechtspersönlichkeit (zB eine Gesellschaft bürgerlichen Rechts gem §§ 1175ff ABGB)³⁵, nicht jedoch eine Hauseigentümergeinschaft, da es sich dabei nicht um eine juristische Person, sondern bloß um eine Zusammenfassung mehrerer Personen handelt.³⁶ Die vormalige Beschränkung des Betroffenen-Begriffes des § 3 Z 2 DSG 1978, nämlich dass juristische Personen des öffentlichen Rechts und deren Organe bei der Besorgung behördlicher Aufgaben nicht als Betroffene galten, wurde aufgegeben.

³³ *Drobesch/Grosinger*, Datenschutzgesetz 118.

³⁴ Vgl § 11a VersVG.

³⁵ *Drobesch/Grosinger*, Datenschutzgesetz 119.

³⁶ DSK 175.284, ZfVBDat 1982/6/11.

Dem Betroffenen iSd DSG 2000 kommen wesentliche Rechte wie zB das Recht auf Geheimhaltung (§ 1 Abs 1), das Recht auf Auskunft (§§ 1 Abs 3 Z 3 bzw 26), das Recht auf Berichtigung und Löschung (§§ 1 Abs 3 Z 2 bzw 27) oder das Recht auf Widerspruch (§ 28) zu. Werden jedoch Daten, die ihn selbst betreffen, vom Auftraggeber verwendet, so entfällt die Betroffeneneneigenschaft für den Auftraggeber in diesem Fall. Eine falsche Schreibweise von Namen oder Adressen reicht jedenfalls nicht dazu aus, die Betroffeneneneigenschaft zu verneinen und somit die Rechte des DSG 2000 zu verweigern.³⁷ Liquidierte bzw rechtlich nicht mehr existente juristische Personen oder verstorbene natürliche Personen sind keine datenschutzrechtlich Betroffenen und genießen daher auch keines der erwähnten Betroffenenrechte.³⁸

3.1.3 Auftraggeber

§ 4 Z 4 definiert den Auftraggeber (und damit den Träger der wesentlichen Pflichten nach dem DSG 2000) als natürliche oder juristische Person, Personengemeinschaft oder Organ einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe (zB Amt der Landesregierung), wenn diese allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten. Dies gilt unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Weiters gilt auch als Auftraggeber, wer einem anderen Daten zur Herstellung eines von ihm aufgetragenen Werkes überlassen hat und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Entscheidend für eine Qualifikation als Auftraggeber sind einzig und allein die faktischen Umstände (die Entscheidung zur Datenverarbeitung), auf die rechtliche Zulässigkeit der Verarbeitung kommt es nicht an. Wurde dem Auftragnehmer jedoch anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder aber hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung aufgrund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gem § 6 Z 4 eigenverantwortlich zu treffen (insbesondere durch Vornahme einer Verarbeitung der überlassenen Daten), so gilt der mit der Herstellung des Werkes Betraute als Auftraggeber iSd DSG 2000. In erster Linie kommen für eine eigenverantwortliche Entscheidung zur Datenverwendung bestimmte freie Berufe

³⁷ OGH 6 Ob 12/85, SZ 59/123 = EDVuR 1986/3, 27 = JBl 1986, 663 = JUS 1986/21, 12 = RdW 1986, 306.

wie Rechtsanwälte, Wirtschaftstreuhandler oder Ziviltechniker in Betracht, um deren Klienten nicht für deren Datenverarbeitungen verantwortlich zu machen³⁹ (allerdings stellt sich die Frage, wie der Betroffene von der Existenz und vom Inhalt solcher Standes- oder Verhaltensregeln Kenntnis erlangen kann⁴⁰, zudem wächst auch der bürokratische Aufwand⁴¹). Auftraggeber ist auch, wer angemietetes Datenmaterial aufgrund eigener Ermittlungen später selbst erweitert.⁴²

Bei Gebietskörperschaften sind sowohl der Rechtsträger als auch dessen Organe datenschutzrechtliche Auftraggeber, bei anderen juristischen Personen als Gebietskörperschaften gilt jedoch nur der Rechtsträger als Auftraggeber iSd DSG 2000. Deren Organe treffen somit mit Wirkung für die juristische Person datenschutzrelevante Entscheidungen (zB der Vorstand einer AG).

Durch die Einbeziehung der Geschäftsapparate der Organe von Gebietskörperschaften sollen auch behördliche Hilfsorgane zum Kreis der Auftraggeber zählen. Durch ihre rechtliche Funktion können sie jedoch weder alleine für sich noch gemeinsam mit anderen die Entscheidung, Daten für einen bestimmten Zweck zu verarbeiten, treffen. Es wurde deshalb die Frage gestellt, ob damit der Kreis der Auftraggeber im Sinne der ErläutRV erweitert wurde.⁴³

3.1.4 Dienstleister

Gem § 4 Z 5 gilt als Dienstleister iSd DSG 2000 jede natürliche oder juristische Person, Personengemeinschaft oder Organ einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, iSd § 4 Z 8 verwenden. Beispiel für einen Dienstleister wäre etwa eine externe EDV-Firma, die vom Auftraggeber überlassene Daten in dessen Namen verarbeitet und die Ergebnisse wiederum an den Auftraggeber liefert. Analog zu den Ausführungen zum datenschutzrechtlichen Auftraggeber treffen auch bei anderen juristischen Personen als

³⁸ *Drobesch/Grosinger*, Datenschutzgesetz 120.

³⁹ *Duschaneck/Rosenmayr-Klemenz*, *ecolex* 1999, 362.

⁴⁰ *Jahnel*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49 (50f).

⁴¹ *Duschaneck*, Neuerungen und offene Fragen im Datenschutzgesetz 2000, ZfV 2000 526 (528).

⁴² OGH 6 Ob 12/85, SZ 59/123 = EDVuR 1986/3, 27 = JBl 1986, 663 = Jus 1986/21, 12 = RdW 1986, 306.

⁴³ *Drobesch/Grosinger*, Datenschutzgesetz 120.

Gebietskörperschaften deren Organe datenrechtliche Entscheidungen mit Wirkung für die juristische Person als Dienstleister.

Nach Art 2 lit e DS-RL ist das entscheidende Kriterium für die Dienstleistereigenschaft die vorherige Weisung zur Verarbeitung durch den Auftraggeber. Dies kommt in § 4 Z 5 weniger deutlich zum Ausdruck und wird erst durch andere Bestimmungen im DSG 2000 verdeutlicht (vgl §§ 11 und 15).

3.1.5 Abgrenzung der Begriffe „Auftraggeber“ und „Dienstleister“

Durch das DSG 2000 wurden die beiden Begriffe „Auftraggeber“ und „Dienstleister“ auch auf Personengemeinschaften und Geschäftsapparate von Organen von Gebietskörperschaften ausgedehnt und es wurde somit einem Wunsch der Praxis entsprochen.⁴⁴ Grundsätzlich ist der Dienstleister nur für die dem Datenschutz entsprechende Durchführung der Verarbeitung, Datensicherung und Erfüllung von Weisungen des Auftraggebers zuständig, wohingegen der Auftraggeber als „Herr der Daten“⁴⁵ vor allem für die rechtliche Zulässigkeit und die Einhaltung der Qualitätsgrundsätze der einzelnen Verarbeitungsschritte verantwortlich ist.

Lange stellte die Abgrenzung zwischen den beiden Begriffen ein Problem dar, wenn die Frage zu klären war, wer die Entscheidung über den Einsatz von EDV treffen muss, um als datenschutzrechtlicher „Auftraggeber“ zu gelten. Nunmehr wird der Einsatz von EDV grundsätzlich dem Auftragserteiler eines Werkes zugerechnet, da in der heutigen Zeit vom Einsatz einer EDV-Anlage auszugehen ist, wenn ein Werk unter Benützung von Daten zu erbringen ist. Eine ausdrückliche Vereinbarung zwischen Auftragserteiler und –beauftragten ist für eine Zurechnung somit nicht nötig.

Anders stellt sich jedoch die Situation dar, wenn der Auftragserteiler dem Auftragsnehmer ausdrücklich den Einsatz von EDV verboten hat: Setzt der Auftragsnehmer dann dennoch EDV ein, so ist er selbst datenschutzrechtlicher Auftraggeber. Der Vorteil dieser Regelung liegt darin, dass die Betroffenenrechte gegenüber jenen Personen zum Tragen kommen, die dieser Rolle auch in der

⁴⁴ ErläutRV 1613 BlgNR 20. GP 37.

Realität gerecht werden können. So wird sich ein Betroffener im Normalfall nicht an den Auftragnehmer wenden können, weil er dessen Identität nicht kennt, um zB ein Auskunftsbegehren zu stellen.

Die Weitergabe von Daten vom Auftraggeber an den Dienstleister stellt keine Übermittlung iSd § 7 dar, vorausgesetzt die Qualitätsgrundsätze des § 6 werden eingehalten – es handelt sich um eine Überlassung, die nicht vom Wirkungskreis des § 7 umfasst ist. Gleiches gilt analog für die Weitergabe von Daten vom Dienstleister an seinen Subunternehmer⁴⁶, der jedoch gem § 11 Abs 1 Z 3 vom Auftraggeber zu billigen ist.

3.1.6 Verwenden von Daten

Die DS-RL sieht in Art 2 lit b einen einzigen Oberbegriff für die verschiedenen Formen der „Verarbeitung“ von personenbezogenen Daten vor, der alle denkmöglichen Verarbeitungsschritte umfasst. In Umsetzung der RL verwendet § 4 Z 8 DSG 2000 den umfassenden Begriff des „Verwendens von Daten“. Sämtliche Schritte des DSG 1978 - Ermitteln, Verarbeiten und Übermitteln – sind in diesem Begriff vereint, was dem Rechtsunterworfenen die Anwendung datenschutzrechtlicher Normen erleichtert. Da dies jedoch nicht dem bisherigen Sprachgebrauch entspricht, werden der österreichischen Rechtstradition folgend auch weiterhin die Begriffe „verarbeiten“ (Z 9), „ermitteln“ (Z 10) und „übermitteln“ (Z 12) unterschieden⁴⁷, die alle – ebenso wie das „Überlassen von Daten“ nach Z 11 - unter den Überbegriff „Verwenden von Daten“ subsumiert werden.

3.2 Der Schutz des Datengeheimnisses durch das DSG 2000

Wie bereits in Kapitel 2.1 erwähnt, wird durch die Verfassungsbestimmung des § 1 Abs 1 jedermann ein Grundrecht auf Datenschutz gewährt, welches auch für juristische Personen und Personengemeinschaften gilt und mit unmittelbarer Drittwirkung ausgestattet ist. Es handelt sich wie bereits erläutert um kein einheitliches Grundrecht, es setzt sich vielmehr aus mehreren Rechten zusammen (siehe Kapitel 2.1). Gem § 3 ist grundsätzlich auf jede Datenverwendung in Österreich österreichisches Recht anzuwenden, zugunsten des Sitzstaatsprinzips

⁴⁵ Dohr/Pollirer/Weiss, Datenschutzrecht², 48.

⁴⁶ Dohr/Pollirer/Weiss, Datenschutzrecht², 53.

⁴⁷ ErläutRV 1613 BlgNR 20. GP 38.

bestehen jedoch Ausnahmen: Werden Daten in Österreich für einen Auftraggeber aus einem anderen EU-Staat verarbeitet, der keine inländische Niederlassung hat, so gilt das Recht des Sitzstaates (so wie auch im umgekehrten Fall das österreichische DSG 2000 im EU-Ausland zur Anwendung kommt, wenn ein österreichischer Auftraggeber keine Niederlassung im Ausland hat). Die Abgrenzung von Auftraggebern des privaten und des öffentlichen Bereiches wird in § 5 geregelt, wobei in Abs 2 definiert wird, welche Auftraggeber als jene des öffentlichen Bereiches gelten (siehe Kapitel 4.1).

Der zweite Abschnitt des DSG 2000 enthält Regelungen, wann die Verwendung personenbezogener Daten zulässig ist. Da im Kapitel 4.5 über die Rechtswidrigkeit ausführlich darauf eingegangen wird, erfolgt hier nur ein kurzer Überblick über diesen Abschnitt: Die Zulässigkeitsvoraussetzungen für die Verarbeitung und Übermittlung von Daten werden in den §§ 6ff formuliert: § 6 enthält eine Reihe von Grundsätzen für die rechtmäßige Verwendung von Daten und in § 7 wird die grundsätzliche Zulässigkeit der Verarbeitung von Daten geregelt, sofern nicht schutzwürdige Geheimhaltungsinteressen des Betroffenen, die in den §§ 8 und 9 näher definiert werden, verletzt werden. Auch wie bereits nach dem DSG 1978 ist es einem Auftraggeber gem § 10 DSG 2000 erlaubt, einen Dienstleister für Datenanwendungen in Anspruch zu nehmen, der allerdings ausreichend Gewähr für eine rechtmäßige und sichere Datenverwendung bieten muss und dessen Pflichten in § 11 normiert sind. Die Überlassung von Daten in das Ausland wird durch die §§ 12 und 13 geregelt: Übermittlungen in andere Mitgliedsstaaten der EU sind demnach grundsätzlich uneingeschränkt zulässig, für einen Datenverkehr in andere Staaten müssen zusätzliche Voraussetzungen vorliegen.

Wie schon nach alter Rechtslage ist der Auftraggeber auch nach dem DSG 2000 durch dessen § 14 dazu verpflichtet, Datensicherungsmaßnahmen zu ergreifen. Nicht nur Vorschriften über die bloße ordnungsgemäße Verwendung von Daten und Vorkehrungen zur Geheimhaltung dieser Daten vor Unbefugten sind darin enthalten, sondern auch Maßnahmen zur Sicherung der Daten vor Verlust oder Zerstörung. Dabei ist der jeweilige Stand der Technik zu berücksichtigen und ein Schutzniveau zu gewährleisten, das den Risiken der jeweiligen Datenverwendung

und der zu schützenden Datenart angemessen ist. Analog zum Bankgeheimnis⁴⁸ enthält § 15 eine Verpflichtung des Auftraggebers, des Dienstleisters und deren Arbeitnehmer zur Wahrung des Datengeheimnisses – Daten, die diesen Personen aufgrund ihrer berufsmäßigen Beschäftigung bekannt oder zugänglich geworden sind, sind (soweit kein rechtlich zulässiger Grund für eine Übermittlung besteht) geheim zu halten. Zudem dürfen Mitarbeiter Daten nur aufgrund einer ausdrücklichen Anordnung ihres Arbeitgebers übermitteln und auch nach Beendigung des Arbeitsverhältnisses ist das Datengeheimnis zu wahren. Eine vorsätzliche Verletzung des Datengeheimnisses stellt zusätzlich einen Verwaltungsstraftatbestand nach § 52 dar.

Verarbeitet ein Auftraggeber personenbezogene Daten, so ist er grundsätzlich dazu verpflichtet, gem § 17 Abs 1 bei der DSK vor Beginn der Verarbeitung eine Meldung zur Registrierung im Datenverarbeitungsregister abzugeben (man beachte die „DVR“-Nummer auf diversen Unterlagen, Rechnungen oder Informationsschriften). Werden sensible Daten, strafrechtlich relevante Daten iSd § 8 Abs 4, Auskunftserteilungen über die Kreditwürdigkeit des Betroffenen oder Daten in Form eines Informationsverbundsystems verwendet, so bedarf es einer Vorabkontrolle durch die DSK. Ansonsten darf der Vollbetrieb einer Datenanwendung gem § 18 Abs 1 sofort nach der Abgabe der Meldung an die DSK aufgenommen werden, sofern es sich nicht ohnehin um eine nicht meldepflichtige Datenanwendung des § 17 Abs 2 handelt. Die am 1. Juli 2000 in Kraft getretene StMV unterscheidet zwischen Standardanwendungen, die meldefrei sind (es handelt sich dabei um bestimmte Typen von Datenanwendungen, die von einer großen Zahl von Auftraggebern in gleichartiger Weise vorgenommen werden und bei denen die Gefahr einer Verletzung schutzwürdiger Interessen Dritter unwahrscheinlich ist, zB Personal- oder Patientenverwaltungen) und Musteranwendungen, die einer vereinfachten Meldepflicht unterliegen (zB Hotel- oder Personentransportreservierung).

Neu im österreichischen Datenschutzrecht ist die in § 24 vorgesehene Informationspflicht des Auftraggebers: Der Auftraggeber einer Datenanwendung hat aus Anlass der Ermittlung von Daten dem Betroffenen in geeigneter Weise

⁴⁸ Vgl § 38 BWG.

über den Zweck der Datenanwendung Auskunft zu geben sowohl für wen die Daten ermittelt werden als auch über den Auftraggeber selbst (Name und Adresse) – auch weitere Informationen (wie zB ein eventuelles Widerspruchsrecht des Betroffenen) sind offenzulegen.

Betroffenen werden durch das DSG 2000 verschiedene Rechte gewährt (die sich nach § 29 allerdings nicht auf nur indirekt personenbezogene Daten beziehen): § 26 normiert ein Recht auf Auskunft, welches grundsätzlich binnen 8 Wochen ab Stellung des Auskunftsbegehrens gewährt werden muss. In bestimmten Fällen (Abs 2) ist der Auskunftsantrag jedoch abzulehnen. Hat der Betroffene nach Ausübung des Auskunftsrechts oder auf andere Weise davon erfahren, dass unrichtige oder unzulässigerweise verarbeitete Daten verwendet wurden, so kann er nach § 27 einen Antrag auf Richtigstellung bzw Löschung stellen. Auch ohne Antrag muss der Auftraggeber Selbiges veranlassen, sobald ihm die Unrichtigkeit oder Unzulässigkeit der Verarbeitung bekannt geworden ist. Nach Beendigung der Datenanwendung gilt die Verwendung der Daten jedenfalls als unzulässig und sind grundsätzlich die Daten zu löschen, sofern eine Archivierung nicht gesetzlich gestattet ist (siehe Kapitel 4.5.1). Ist die Verwendung von Daten nicht gesetzlich vorgesehen, so verleiht § 28 dem Betroffenen ein Widerspruchsrecht: Jeder Betroffene hat 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. Liegen diese Voraussetzungen vor, so hat der Auftraggeber jegliche Übermittlung der Daten zu unterlassen und diese binnen acht Wochen zu löschen. Gegen eine andere als die gesetzlich angeordnete Aufnahme in ein öffentliches Register (zB Telefonbuch-CDs, mit deren Hilfe nicht nur vom Namen auf die Telefonnummer geschlossen werden kann, sondern auch umgekehrt ein Rückschluss von der Nummer auf den Namen möglich ist⁴⁹) kann gem Abs 2 jederzeit auch ohne Begründung Widerspruch erhoben werden.

Die schadenersatzrechtliche Bestimmung enthält § 33, die den Schwerpunkt dieser Arbeit bildet und auf die im Folgenden anhand der allgemeinen

⁴⁹ Souhrada-Kirchmayer, SozSi 2000, 949.

Bestimmungen des Schadenersatzrechts und der sich ergebenden datenschutzrechtlichen Besonderheiten näher eingegangen wird.

4. Schadenersatz im DSG 2000

4.1 Abgrenzung öffentlicher – privater Bereich

Wie bereits das DSG 1978 unterscheidet auch das DSG 2000 zwischen einem öffentlichen und einem privaten Teil. In § 5 Abs 2 sind diejenigen Auftraggeber angeführt, die als Auftraggeber des öffentlichen Rechts gelten (es sind dies Auftraggeber, die in Formen des öffentlichen Rechts eingerichtet sind und solche, die trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind). Alle anderen Auftraggeber gelten nach der Generalklausel des Abs 3 datenschutzrechtlich als Auftraggeber des privaten Bereichs. Wesentlich ist die Unterscheidung zwischen diesen beiden Formen der Auftraggeberschaft vor allem für den Bereich des Rechtsschutzes: Dieser obliegt gem § 1 Abs 5 für den öffentlichen Bereich der DSK und (mit Ausnahme des Rechtes auf Auskunft) für den privaten Bereich den ordentlichen Gerichten. Damit wird das Grundrecht auf Datenschutz (einmalig im österreichischen Rechtssystem) mit unmittelbarer Drittwirkung ausgestattet und folglich ist die Geltendmachung von Schadenersatzansprüchen nach § 33 DSG 2000 auf jene Fälle beschränkt, in denen der Auftraggeber dem privaten Bereich zugerechnet wird. Handelte der (grundsätzlich dem öffentlichen Bereich zugerechnete) Rechtsträger allerdings im Bereich der Privatwirtschaftsverwaltung, so kommt ebenfalls § 33 DSG 2000 zur Anwendung.⁵⁰ Für Fehlleistungen durch Auftraggeber öffentlichen Rechts im Bereich der Gerichtsbarkeit oder der Hoheitsverwaltung kommt die Amtshaftung in Betracht (siehe Kapitel 6). Die eigentliche Verweisung auf den Zivilrechtsweg erfolgt durch § 33 Abs 1: *„Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen des DSG 2000 verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen“*. Somit kommen grundsätzlich die Bestimmungen der §§ 1293ff ABGB zur Anwendung.

⁵⁰ Schragel, Kommentar zum Amtshaftungsgesetz³ (2003) Rz 13.

4.2 Allgemeines zum Schadenersatz

Im österreichischen Rechtssystem gilt der Grundsatz, dass ein Schaden denjenigen trifft, in dessen Vermögen oder Person er sich ereignet⁵¹; der Schaden ist also grundsätzlich selbst zu tragen. Bei Vorliegen von bestimmten Voraussetzungen wird dieser Grundsatz durchbrochen und der Schaden ist von demjenigen zu tragen, dem der in der Rechtssphäre eines anderen entstandene Schaden objektiv zurechenbar ist. *„Das Schadenersatzrecht ist die Summe der Vorschriften, die regeln, wann ein Geschädigter bei ihm eingetretenen Schaden von jemand anderem ersetzt verlangen kann.“*⁵² Folgende Voraussetzungen müssen gegeben bzw erfüllt sein, damit es zu einer Überwälzung des Schadens kommen kann:

- Schaden
- Kausalität
- Rechtswidrigkeit
- Rechtswidrigkeitszusammenhang
- Verschulden

Unter diesen Gesichtspunkten ist auch der weitere Verlauf dieser Arbeit gestaltet, wobei sich die Ausführungen auf diejenigen Bereiche konzentrieren werden, die für den Schadenersatz nach Verletzungen des Datengeheimnisses von besonderer Bedeutung sind.

4.3 Schaden

Grundvoraussetzung für jegliche Art von Schadenersatz ist das Vorliegen eines Schadens, der als „jeder Nachteil, der jemandem an Vermögen, Rechten oder an der Person zugefügt worden ist“⁵³ in § 1293 ABGB definiert wird. Ein Schaden kann materiell oder immateriell sein: Ersterer (Vermögensschaden) ist ein Nachteil im Vermögen der geschädigten Person und lässt sich in einer genau bezifferbaren Summe von Geld oder anderen vertretbaren Sachen ausdrücken.

⁵¹ Koziol/Welser, Grundriss des bürgerlichen Rechts II¹² (2001) 282.

⁵² Koziol/Welser, Grundriss II¹², 282.

⁵³ Harrer in Schwimann, Praxiskommentar zum ABGB VII² (1997) § 1293 Rz 1.

Immaterielle Schäden sind nicht in Geld messbar und werden nur in denjenigen Fällen ersetzt, in denen dies ausdrücklich gesetzlich vorgeschrieben ist.⁵⁴ Es handelt sich insbesondere um Fälle von Schmerzensgeld (§ 1325), Verletzung der geschlechtlichen Selbstbestimmung (§ 1328), Wert der besonderen Vorliebe (§ 1331), Freiheitsentziehung (§ 1329) und andere, gesetzlich geregelte Fälle. Eine dieser immateriellen Schadenersatz vorsehenden Normen ist § 33 Abs 1 2. Satz DSG 2000, auf die im Folgenden näher einzugehen sein wird.

4.3.1 Materielle Schäden

Im Anwendungsbereich des DSG 2000 ist eine breite Palette von Fällen denkbar, in denen sich der eingetretene Schaden in Geld oder anderen vertretbaren Sachen messen lässt. So kann sich beispielsweise der Schaden darin manifestieren, dass die Krankengeschichte eines Arbeitnehmers unzulässigerweise vom EDV-Dienstleister des Krankenhauses an den Arbeitgeber übermittelt wird und dieser in der Folge den Arbeitnehmer kündigt oder nicht befördert, was (im Hinblick auf ein höheres Gehalt) ein entgangener Gewinn wäre. Auch kann etwa ein Auftraggeber einem Hacker den Auftrag erteilen, über das Internet in ein Computernetzwerk einzudringen und sensible Daten auszuspionieren um diese später in Gewinnerzielungsabsicht zu verkaufen, wobei den Betroffenen durch die unzulässige Verwendung ihrer Daten ein Schaden entstehen kann. In der Regel werden Schadenersatzansprüche aus § 33 wohl meist auf den Ersatz von materiellen Schäden gerichtet sein.

4.3.2 Immaterielle Schäden

In Fällen von schwerwiegenden und rechtswidrigen Datenverwendungen, die Tatbeständen vergleichbar sind, die nach dem MedG zum Schadenersatz verpflichten, kann der Betroffene nunmehr seit dem Inkrafttreten des DSG am 1.1.2000 immaterielle Schadenersatzansprüche auf § 33 Abs 1 zweiter Satz stützen. Näheres hierzu unter Kapitel 4.10.

⁵⁴ *Koziol/Welser, Grundriss II*¹², 306.

4.4 Kausalität

Grundvoraussetzung für eine eventuelle Überwälzung des Schadens ist, dass das Verhalten des Schädigers überhaupt kausal für den Schadenseintritt war. Die Kausalität eines Verhaltens wird mit zwei Theorien überprüft:

Einerseits wird mit Hilfe der Äquivalenztheorie geprüft, ob der Erfolg (Eintritt des Schadens) überhaupt ohne das Verhalten des Schädigers eingetreten wäre. War das Verhalten nicht *conditio sine qua non*, so war es auch nicht kausal. Andererseits müssen die Resultate der Äquivalenztheorie eingeschränkt werden, da es ansonsten zu einer zu weitreichenden Haftung für Schäden kommen würde. Dies geschieht mit Hilfe der Adäquanztheorie: Die Kausalität wird für diejenigen Schadensfälle ausgeschlossen, in denen das Verhalten des Schädigers einen völlig unvorhergesehenen Erfolg herbeigeführt hat.⁵⁵

Auf das DSG 2000 bezogen wäre etwa nach der *conditio sine qua non*-Theorie das Herstellen eines PCs durch einen Fabrikanten kausal für einen Schaden, den ein Computer-Hacker durch die unbefugte Erlangung und Veröffentlichung personenbezogener Daten unter Benützung eines Modells dieses Herstellers verursacht hat (ohne PC hätte der Hacker schließlich kein Werkzeug gehabt und somit auch keinen Schaden verursachen können). Die Adäquanztheorie würde den Hersteller des PCs jedoch (abgesehen von den weiteren Voraussetzungen für die Überwälzung des Schadens) von der Haftung befreien, da der Hersteller des PCs mit dem Eintritt des Schadens nicht vernünftigerweise rechnen konnte.

4.5 Rechtswidrigkeit

Ein menschliches Verhalten ist rechtswidrig, wenn es entweder gegen Ge- oder Verbote oder gegen die guten Sitten verstößt (für eine vertragliche Haftung ist das vertragswidrige Verhalten rechtswidrig).⁵⁶ Die Rechtswidrigkeit ist bei verschuldensabhängigen Delikten wie dem (deliktischen oder vertraglichen) Schadenersatz von Relevanz, da es bei den verschuldensunabhängigen Delikten auf die Schaffung einer potentiell gefährlichen Situation und nicht auf ein rechtswidriges Verhalten des Einzelnen ankommt.

⁵⁵ *Koziol/Welser, Grundriss II*¹², 290ff.

Die Verwendung von Daten (und somit diejenigen Fälle, in denen nicht datenschutzrechtswidrig gehandelt wird) wird im zweiten Abschnitt des DSG 2000 geregelt, dabei wird grundsätzlich vom Verbotsprinzip ausgegangen: Personenbezogene Daten dürfen nur verarbeitet werden, falls eine rechtliche Ermächtigung dazu vorliegt. Eine nach dem DSG 2000 unzulässige Verarbeitung von Daten ist demnach grundsätzlich rechtswidrig iSd Schadenersatzrechts. Wann eine solche Verarbeitung von Daten nach dem DSG 2000 zulässig ist wird im folgenden Kapitel dargestellt.

4.5.1 Grundsätze

Ausdruck des Verbotsprinzips ist der Katalog des § 6, der fünf grundsätzliche Bedingungen für eine rechtmäßige Verwendung von personenbezogenen Daten enthält. Gem § 6 Abs 1 Z 1 dürfen Daten demnach nur nach Treu und Glauben und zudem auch noch nur auf rechtmäßige Weise verwendet werden, dh der Auftraggeber muss die rechtliche Befugnis für die Benützung der Daten besitzen. Die „Rechtmäßigkeit“ bezieht sich nicht nur auf das DSG 2000 allein, sondern auch auf bereichsspezifische Datenschutzregelungen⁵⁷ wie etwa die Datenschutzgesetze der Länder. Zudem darf der Betroffene bezüglich der Umstände des Datengebrauchs, des Bestehens und der Durchsetzbarkeit seiner Rechte auch nicht im Unklaren gelassen oder gar irregeführt werden.⁵⁸

Nach Z 2 dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt werden, zudem darf eine allfällige Weiterverwendung nicht mit diesen Zwecken kollidieren (eine Weiterverwendung für wissenschaftliche Zwecke ist nach Maßgabe der §§ 46 und 47 jedoch erlaubt).

Z 3 normiert einen Zweckbindungsgrundsatz: Die Verwendung von Daten ist nur zulässig, soweit sie für den Zweck der Datenanwendung wesentlich ist und auch nicht über diesen Zweck hinausgeht. Es wird daher zu untersuchen sein, ob alle Daten wirklich benötigt werden – die Anlegung eines „Datenvorrats“ für eine

⁵⁶ *Koziol/Welser*, Grundriss II¹², 293.

⁵⁷ *Duschaneck/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) § 6 Pkt 2.1.

⁵⁸ ErläutRV 1613 BlgNR 20. GP 39.

eventuelle spätere Verwendung ist somit jedenfalls nicht zulässig⁵⁹ und Unklarheiten in der Festlegung des Zwecks gehen zu Lasten des Auftraggebers.

Daten müssen nach Z 4 im Ergebnis sachlich korrekt und erforderlichenfalls auf den letzten Stand gebracht verwendet werden. Hat etwa eine Datenanwendung ein „Verzeichnis von Straftätern“ zum Zweck, so dürfen Personen, die nur einer strafbaren Tat verdächtigt werden, nicht in das Verzeichnis aufgenommen werden⁶⁰ und Bonitätsdaten eines Betroffenen sind stets auf dem neuesten Stand zu halten.

Auf eine allfällige Archivierung bezieht sich Z 5: Daten dürfen nur solange in personenbezogener Form aufbewahrt oder archiviert werden, solange dies für den Zweck der Ermittlung erforderlich ist. Eine allfällige längere Aufbewahrung kann sich jedoch aus anderen gesetzlichen Vorschriften⁶¹ ergeben.

Die Abs 2 und 3 erlegen dem Auftraggeber zusätzliche Pflichten auf: Diesem obliegt gem § 6 Abs 2 stets die Verantwortung zur Einhaltung der oben geschilderten Qualitäts-Grundsätze - auch für den Fall, dass er einen Dienstleister zur Verarbeitung der Daten hinzuziehen sollte. Weiters hat ein Auftraggeber ohne Niederlassung in einem Mitgliedsstaat der EU in Umsetzung von Art 4 Abs 2 DS-RL bei Abgabe der Meldung nach § 19 Abs 1 Z 1 einen im Inland ansässigen Vertreter zu benennen, der bei datenschutzrechtlichen Verstößen zur Verantwortung gezogen werden kann, sollte dies beim Auftraggeber selbst nicht möglich sein.

Zur Präzisierung dessen, was im privaten Bereich als Verwendung nach Treu und Glauben anzusehen ist, können gem § 6 Abs 4 gesetzliche Interessensvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Diese Regeln, die vor einer Veröffentlichung dem Bundeskanzler zur Begutachtung vorgelegt werden müssen,

⁵⁹ VfGH 28.11.2001, B 2271/00; *Dohr/Pollirer/Weiss*, Datenschutzrecht², 68.

⁶⁰ ErläutRV 1613 BlgNR 20. GP 39.

⁶¹ Vgl va das Bundesarchivgesetz, BGBl I 1999/162, die StMV, § 10 Abs 1 Z 3 KAKuG und § 51 Abs 3 ÄrzteG 1998.

haben allerdings keinen verbindlichen Charakter⁶² und können am ehesten mit den ÖNormen verglichen werden.⁶³

4.5.2 Zulässigkeit der Verwendung von Daten

Ein weiterer Ausdruck des Verbotsprinzips ist die Regelung des § 7: Demnach dürfen Daten nur verarbeitet werden, „soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind“ und zudem (als zweite Voraussetzung) auch die schutzwürdigen Geheimhaltungsinteressen des Betroffenen (§§ 8 und 9) nicht verletzt werden. Der Gesetzgeber will somit im Falle der Verarbeitung personenbezogener Daten durch einen Privaten auf den von der Rechtsordnung anerkannten Zweck des privaten Rechtsträgers abstellen (im öffentlichen Bereich leitet sich die Berechtigung zur Verarbeitung aus den Materiengesetzen ab). Im Einzelfall wird der Private also nachzuweisen haben, dass ein vom Gesetz her gebilligter Grund für die Verarbeitung von Daten vorliegt bzw eine Situation, die die Verarbeitung der Daten rechtfertigt. Eine solche Berechtigung könnte sich beispielsweise aus einer Gewerbeberechtigung, aus den Vereinsstatuten, aus dem Gesellschaftsvertrag oder aus Regelungen über die Ausübung bestimmter Berufe ableiten lassen, wobei nicht nur die konkrete Berechtigung, sondern die Rechtsordnung als Gesamtheit als Prüfungsmaßstab heranzuziehen ist.⁶⁴ Grundvoraussetzung einer jeglichen Datenverwendung ist nach § 7 Abs 3 jedoch, dass die damit verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit dem gelindesten zur Verfügung stehenden Mitteln erfolgen sowie weiters, dass die in § 6 normierten Grundsätze eingehalten werden. Für eine Übermittlung von Daten legt § 7 Abs 2 fest, dass diese nur übermittelt werden dürfen, wenn sie aus einer gem Abs 1 zulässigen Datenanwendung stammen, wenn weiters der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und (kumulativ) durch den Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Die Beurteilung des Vorliegens der Umstände, die eine Übermittlung zulässig machen, obliegt

⁶² ErläutRV 1613 BlgNR 20. GP 40.

⁶³ Mayer-Schönberger/Brandl, Datenschutzgesetz 2000 24; Drobesch/Grosinger, Datenschutzgesetz 132.

⁶⁴ Dohr/Pollirer/Weiss, Datenschutzrecht², 72.

dem Übermittler – werden Daten ohne Ersuchen übermittelt, so darf der Übermittelnde keinen Zweifel am Vorliegen dieser Umstände haben.⁶⁵ Im Normalfall wird die ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis des Empfängers von übermittelten Daten außer Zweifel stehen und eine Glaubhaftmachung wird entfallen können. *Dohr/Pollirer/Weiss*⁶⁶ gehen davon aus, dass ein Nachweis der Berechtigung bei Übermittlung von zulässigerweise veröffentlichten Daten, bei indirekt personenbezogenen Daten sowie bei einer gesetzlichen Verpflichtung zur Datenübermittlung gänzlich entfallen kann. Aus der Auskunftspflicht des Auftraggebers nach § 26 über die Herkunft von Daten und der Offenlegungspflicht nach § 24 bei Übermittlungen und Mitteilungen an Betroffene ergibt sich die Verpflichtung des Übermittlers (sofern nicht ohnehin schon bekannt), seine Identität in geeigneter Weise dem Empfänger offen zu legen. Anonyme Übermittlungen sind nur in Ausnahmesituationen zulässig.⁶⁷

4.5.3 Schutzwürdige Geheimhaltungsinteressen bei Verwendung von nicht-sensiblen Daten

Der Gesetzgeber hat durch den Katalog des § 8 Abs 1 festgelegt, wann schutzwürdige Interessen bei der Verwendung von nicht-sensiblen Daten nicht verletzt werden: Es handelt sich dabei um Fälle einer ausdrücklichen gesetzlichen Ermächtigung oder Verpflichtung zur Verwendung der Daten⁶⁸ (wobei der Begriff „Verwendung“ jede Handhabung von Daten beinhaltet, also auch das Ermitteln und Übermitteln von Daten) sowie Fälle einer jederzeit widerrufbaren Zustimmung des Betroffenen zur Verwendung (ein Widerruf macht jedoch eine bereits erfolgte Datenverwendung nicht rückwirkend unzulässig⁶⁹; ein gesetzliches Verbot zur Datenübermittlung wirkt jedoch absolut und kann auch durch die Zustimmung des Betroffenen nicht beseitigt werden⁷⁰) Weiters erfasst sind Fälle, in denen lebenswichtige Interessen des Betroffenen die Verwendung erfordern sowie Situationen, in denen vertraglich begründete⁷¹ überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erforderlich machen (§ 8 Abs 3 führt demonstrativ Beispiele dafür an).

⁶⁵ *Drobesh/Grosinger*, Datenschutzgesetz 134.

⁶⁶ *Dohr/Pollirer/Weiss*, Datenschutzrecht², 72.

⁶⁷ *Drobesh/Grosinger*, Datenschutzgesetz 135.

⁶⁸ Vgl § 18 MeldeG, § 57 SPG.

⁶⁹ *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz § 8 Pkt 2.

⁷⁰ DSK 15.5.2001, K120.713/005-DSK/2001, RIS.

Zwei Ausnahmetatbestände, die eine Verletzung schutzwürdiger Geheimhaltungsinteressen ausschließen, werden in Abs 2 normiert: Es handelt sich zum einen um eine Verwendung von zulässigerweise veröffentlichten Daten und zum anderen um bloß indirekt personenbezogene Daten, bei denen ein Personenbezug mit rechtlich zulässigen Mitteln vom Verwender nicht mehr herstellbar ist. Im Falle der Verwendung von zulässigerweise veröffentlichten Daten ist jedoch darauf zu achten, ob die Datenanwendung tatsächlich nur diesbezügliche Daten enthält (wie beispielsweise ein Telefonbuch) oder ob nicht auch zusätzliche, bisher nicht veröffentlichte Daten enthalten sind. Um in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen nicht zu verletzen wird zudem auch ausdrücklich auf das Widerspruchsrecht des § 28 verwiesen.

Für die Verwendung gerichtlich oder verwaltungsbehördlich strafbarer Handlungen zieht schließlich § 8 Abs 4 enge Grenzen. Erfasst werden nicht nur Daten über strafrechtliche Verurteilungen, sondern auch Informationen über bloße Tatverdächtige, Angeklagte oder Beschuldigte sowie auch Verwaltungstrafrecht-Delikte.

4.5.4 Schutzwürdige Geheimhaltungsinteressen bei Verwendung von sensiblen Daten

Hinsichtlich der Verwendung von sensiblen Daten bestimmt § 9 in einer taxativen Aufzählung (die weitgehend durch Art 8 DS-RL vorgegeben ist), in welchen Situationen schutzwürdige Interessen des Betroffenen nicht verletzt sind. Es handelt sich dabei ua um Fälle, in denen die Daten offenkundig durch den Betroffenen selbst öffentlich gemacht wurden, in denen die Daten in nur indirekt personenbezogener Form verwendet werden oder sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese zur Wahrung eines wichtigen öffentlichen Interesses dienen. Die Verarbeitung oder Übermittlung von Daten ist weiters zulässig, wenn diese zur Wahrung lebenswichtiger Interessen des Betroffenen nötig ist und dessen Zustimmung nicht mehr rechtzeitig eingeholt werden kann. In Fällen, die nicht unter einen

⁷¹ *Drobesch/Grosinger*, Datenschutzgesetz 139.

Tatbestand des § 9 subsumiert werden können, ist ein schutzwürdiges Geheimhaltungsinteresse bei einer Verwendung von sensiblen Daten grundsätzlich verletzt und macht deren Verwendung somit unzulässig (*Jahnel*⁷² weist darauf hin, dass die DS-RL hinsichtlich mehrerer Tatbestände unrichtig umgesetzt worden ist).

4.5.5 Dienstleistung im Datenverkehr

Der Auftraggeber muss die Daten nicht selbst verarbeiten, sondern er kann sich gem § 10 auch eines Dritten, des Dienstleisters, bedienen. Dieser muss allerdings ausreichend Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat die dafür nötigen Vereinbarungen (in der Regel in Werkvertragsform) mit dem Dienstleister zu treffen und muss sich weiters von ihrer Einhaltung durch den Dienstleister überzeugen. Dadurch soll der Auftraggeber zu einer sorgfältigen Auswahl des Dienstleisters angehalten werden; der Auftraggeber hat entsprechende Informationen vor Vertragsabschluss einzuholen. Tauchen beim Auftraggeber Zweifel über die Zuverlässigkeit seines Dienstleisters auf oder besteht das Dienstleistungsverhältnis auf längere Zeit, so hat eine erneute Prüfung durch den Auftraggeber stattzufinden.⁷³ Die in Abs 2 vorgesehene Mitteilungspflicht an die DSK betrifft nur Auftraggeber des öffentlichen Bereichs und kann daher (ausgenommen hinsichtlich der Privatwirtschaftsverwaltung) für Fälle des Schadenersatzes gem § 33 außer Acht gelassen werden, da hier der Auftraggeber dem privaten Bereich zugerechnet werden muss.

Wurde ein Dienstleister mit einer Datenanwendung betraut, so erlegt ihm § 11 Abs 1 - unabhängig von eventuellen vertraglichen Vereinbarungen zwischen ihm und dem Auftraggeber - folgende Pflichten auf:

Nach Z 1 darf eine Verwendung der Daten ausschließlich im Rahmen der Aufträge des Auftraggebers erfolgen – eine darüber hinausgehende Verwendung und insbesondere Übermittlung ist nicht zulässig. Zudem dürfen gem Z 2 nur solche Mitarbeiter des Dienstleisters herangezogen werden, die sich zur Einhaltung des Datengeheimnisses nach § 15 verpflichtet haben.

⁷² *Jahnel*, wbl 2000, 52.

⁷³ *Drobesch/Grosinger*, Datenschutzgesetz 149.

Nach *Duschaneck/Rosenmayr-Klemen*⁷⁴ könnte eine solche Erklärung wie folgt aussehen:

Verpflichtungserklärung gem § 15 Abs 2 DSGVO 2000

Ich verpflichte mich, personenbezogene Daten aus Datenanwendungen, die mir zugänglich geworden sind, geheim zu halten soweit kein rechtlich zulässiger Grund für eine Übermittlung besteht. Ich verpflichte mich, Daten nur aufgrund einer ausdrücklichen Anordnung zu übermitteln (und nehme die für meinen Arbeitsplatz geltenden allgemeinen Übermittlungsanordnungen sowie die Liste anordnungsbefugter Personen zur Kenntnis).

Ich verpflichte mich, das Datengeheimnis auch nach Beendigung des Dienstverhältnisses einzuhalten und nehme zur Kenntnis, dass ein Verstoß dagegen nicht nur arbeitsrechtliche, sondern auch (verwaltungs)strafrechtliche Folgen haben kann und allenfalls schadenersatzpflichtig machen kann.

Der Aufbau der Datensicherung ist grundsätzlich Sache des Arbeitgebers und der mit der Softwareentwicklung beauftragte Arbeitnehmer hat nur für die Einhaltung der vorgegebenen Weisungen einzustehen⁷⁵, zudem sind noch alle gemäß § 14 erforderlichen Datensicherungsmaßnahmen zu treffen.

Weitere (Sub)Dienstleister dürfen nach Z 3 nur mit Billigung des Auftraggebers hinzugezogen werden und zudem muss der Auftraggeber so rechtzeitig darüber informiert werden, damit er dies – gegebenenfalls - untersagen kann. Gem Z 4 müssen die Voraussetzungen für die Erfüllung der Auskunft-, Richtigstellungs-, und Löschungspflicht des Auftraggebers zwischen Auftraggeber und Dienstleister koordiniert werden und nach Z 5 sind nach Beendigung des Dienstleistungsverhältnisses alle Daten und Verarbeitungsergebnisse entweder dem Auftraggeber zu übergeben, in dessen Auftrag aufzubewahren oder zu vernichten. All jene Informationen, die der Auftraggeber für die Kontrolle der

⁷⁴ *Duschaneck/Rosenmayr-Klemen*, Datenschutzgesetz 194.

⁷⁵ OGH 9 Ob A 182/90, EDVuR 1990/4, 142 = RdW 1991, 87.

Einhaltung der in Z 1 bis 5 normierten Pflichten benötigt, hat der Dienstleister gem Z 6 bereitzustellen.

4.5.6 Überlassung von Daten in das Ausland

Hinsichtlich des Datenverkehrs mit dem Ausland sind die §§ 12 und 13 von Bedeutung: Eine Überlassung von Daten in einen Mitgliedsstaat der EU ist grundsätzlich keinen datenschutzrechtlichen Beschränkungen unterworfen, was Art 1 Abs 2 DS-RL entspricht: Ein wesentlicher Regelungsgegenstand der DS-RL war es nämlich, den freien Verkehr personenbezogener Daten zwischen den Mitgliedsstaaten nicht zu behindern und Wettbewerbsverzerrungen sowie dadurch mögliche Risiken einer Standortverlagerung zu beseitigen.⁷⁶ Davon nicht erfasst sind allerdings Daten der „dritten Säule“ der EU (Polizeiliche und Justizielle Zusammenarbeit in Strafsachen), da dieser Bereich nicht von der Richtlinie umfasst ist, was im Hinblick auf Schadenersatz im privaten Bereich jedoch zu vernachlässigen ist. Hinsichtlich der Daten juristischer Personen besteht ebenfalls keine Harmonisierung des Datenschutzniveaus in den Mitgliedsstaaten, ein unbeschränkter Datenverkehr in das EU-Ausland erscheint jedoch gerechtfertigt, da in den anderen Mitgliedsstaaten ebenfalls Regelungen bestehen, die im Vergleich zum österreichischen Datenschutzniveau keine gravierenden Nachteile befürchten lassen.⁷⁷

Der Datenverkehr in Drittländer ist nach § 12 Abs 2 nur genehmigungsfrei gestattet, wenn das jeweilige Drittland ein angemessenes Datenschutzniveau bietet. Gem § 1 DSAV sind dies derzeit lediglich die Schweiz und Ungarn. Damit soll verhindert werden, dass ein Auftraggeber personenbezogene Daten im Ausland verarbeiten lässt und diese danach wieder importiert, um sich des Wirkungsbereichs des DSG 2000 zu entziehen. Für Staaten ohne angemessenes Datenschutzniveau gibt es in § 12 Abs 3 jedoch zahlreiche Ausnahmetatbestände. Es handelt sich dabei ua um Fälle einer zulässigen Veröffentlichung im Inland, um nur indirekt personenbezogene Daten, um Übermittlungen aufgrund von Normen in Gesetzesrang oder um Übermittlungen aus Datenanwendungen, die gem § 17 Abs 3 von der Meldepflicht ausgenommen sind. In Abs 3 ist eine „Notfallsregelung“ enthalten: Ist eine Übermittlung bzw Überlassung von Daten in

⁷⁶ Ghali, Datenschutz 237.

das Ausland nicht nach den Abs 1 bis 3 genehmigungsfrei und entweder zur Wahrung eines wichtigen öffentlichen Interesses oder zur Wahrung eines lebenswichtigen Interesses einer Person so dringend, dass die erforderliche Genehmigung der DSK nicht mehr rechtzeitig eingeholt werden kann, so darf die Übermittlung ins Ausland auch ohne Genehmigung vorgenommen werden – dies muss jedoch unverzüglich der DSK mitgeteilt werden, was einer nachträglichen Genehmigung gleichkommt.⁷⁸ Voraussetzung für die datenschutzrechtliche Zulässigkeit eines jeden Datenverkehrs ins Ausland ist gem Abs 5 jedoch die Rechtmäßigkeit der Verwendung der Daten im Inland (§§ 6 und 7). Zudem muss sich der ausländische Dienstleister auch zur Einhaltung der Dienstleisterpflichten nach § 11 Abs 1 verpflichtet haben, da diese Norm außerhalb Österreichs naturgemäß keine Geltung entfalten kann und es somit einer vertraglichen Vereinbarung zwischen dem Auftraggeber und dem ausländischen Dienstleister bedarf. Diese Verpflichtung kann entfallen, falls die Dienstleistung im Ausland in unmittelbar anwendbaren und in Gesetzesrang stehenden Normen vorgesehen ist.⁷⁹

Ist die Ausfuhr von Daten ins Ausland nicht gem § 12 genehmigungsfrei, so ist hierfür nach § 13 Abs 1 eine Genehmigung der DSK nötig, die sowohl für die einmalige als auch für die mehrmalige Überlassung von Daten erteilt werden kann. Diese Genehmigung ist gem Abs 2 zu erteilen, falls nach Abwägung aller Einzelheiten (unbeachtet des Fehlens eines generell angemessenen Datenschutzniveaus im Empfängerstaat) im konkreten Einzelfall ein angemessener Datenschutz besteht oder der Auftraggeber glaubhaft macht, dass die schutzwürdigen Geheimhaltungsinteressen der Betroffenen auch im Ausland ausreichend geschützt werden, wobei es dabei auf die tatsächliche Durchsetzbarkeit entsprechender Vereinbarungen ankommt.⁸⁰ Analog zu § 12 Abs 5 ist auch für jede genehmigungspflichtige Überlassung von Daten ins Ausland Voraussetzung, dass die Datenanwendung bereits im Inland gem §§ 6 und 7 zulässig ist.⁸¹ Das Vorliegen sämtlicher Kriterien ist von der DSK im

⁷⁷ ErläutRV 1613 BlgNR 20. GP 42.

⁷⁸ *Drobesch/Grosinger*, Datenschutzgesetz 157.

⁷⁹ Vgl Art 92 SDÜ.

⁸⁰ *Duschaneck/Rosenmayr-Klemen*z, Datenschutzgesetz § 13 Pkt 7.

⁸¹ *Ghali*, Datenschutz 162; *Duschaneck/Rosenmayr-Klemen*z, Datenschutzgesetz § 13 Pkt 3.

Anzeigeverfahren zu prüfen⁸²; die Entscheidung der DSK erfolgt schließlich mittels Bescheid, der auch Bedingungen und Auflagen enthalten kann.

4.5.7 Rechtfertigungsgründe

Es ist auch die Frage zu klären, ob eine grundsätzlich rechtswidrige Handlung nicht durch einen Rechtfertigungsgrund gedeckt sein kann. Etwaige Zeugenpflichten in behördlichen Verfahren⁸³ ermächtigen zur Übermittlung anvertrauter oder zugänglich gewordener Daten und zum Bruch des Datengeheimnisses. Es kommen jedoch noch andere Rechtfertigungsgründe in Betracht:

4.5.7.1 Notwehr

Es handelt sich hierbei um die Abwehr eines gegenwärtigen oder unmittelbar drohenden rechtswidrigen Angriffes auf ein notwehrfähiges Gut (Leben, Gesundheit, Freiheit, Eigentum), die das erforderliche Maß nicht überschreitet.⁸⁴ Ein rechtswidriges Verhalten ist gem § 19 ABGB rechtmäßig (und führt somit zu keiner Ersatzpflicht), wenn es in Notwehr geschieht.

4.5.7.2 Notstand

Im Notstand handelt derjenige, der zur Abwehr einer unmittelbar drohenden Gefahr in die Rechtsgüter (zum Unterschied zur Notwehr ist auch die Ehre vom Notstands-Begriff umfasst) eines unbeteiligten Dritten eingreift.⁸⁵ Wiegen die Interessen des im Notstand Befindlichen schwerer als jene des Geschädigten, so wird die Rechtswidrigkeit ausgeschlossen und es kommt gem § 1306a ABGB zu einer Billigkeitshaftung. Rechtmäßig ist eine Notstandshandlung nur dann, wenn sie zum Schutz von Gütern gesetzt wurde, die die Rechtsordnung als schutzwürdig anerkennt; die Schutzwürdigkeit ergibt sich daraus, ob das Gut gegenüber Eingriffen Dritter von der Rechtsordnung geschützt wird.⁸⁶

⁸² JAB 2028 BlgNR 20. GP 2.

⁸³ Vgl § 150 StPO, § 48 AVG.

⁸⁴ Vgl § 3 StGB.

⁸⁵ *Koziol/Welser*, Grundriss II¹², 295.

⁸⁶ *Koziol*, Österreichisches Haftpflichtrecht I³ (1997) Rz 4/81.

4.5.7.3 Selbsthilfe

Ein an sich rechtswidriges Verhalten kann durch die Selbsthilfe gerechtfertigt werden, wenn es um die Durchsetzung eines eigenen Rechtes geht und behördliche Hilfe zu spät käme (§§ 19, 344 ABGB).

4.5.7.4 Einwilligung des Verletzten

Ein grundsätzlich rechtswidriges Verhalten kann durch die Einwilligung des Verletzten gerechtfertigt sein, allerdings muss dieser über das gefährdete oder verletzte Rechtsgut frei disponieren können, andernfalls ist die Einwilligung nicht wirksam.⁸⁷ Eine Zustimmung zur Verwendung von personenbezogenen Daten ist in den §§ 8 Abs 1 Z 2 und 9 Z 6 vorgesehen, wobei ein Widerruf jederzeit möglich ist.

In den angeführten Fällen wird man trotz der Verletzung einschlägiger Vorschriften des DSG 2000 (abgesehen von der Einwilligung des Betroffenen, die ja im DSG 2000 direkt geregelt ist) von einer Schadenersatzpflicht befreit.

4.5.8 Überblick über die Rechtswidrigkeit

Zusammenfassend ist zu sagen, dass im DSG 2000 ein rechtswidriges Verhalten nicht ausdrücklich normiert ist – nach dem oben dargestellten Verbotsprinzip sind all jene Handlungsweisen angeführt, die die Verwendung von personenbezogenen Daten zulässig machen.

Im deliktischen Bereich des Schadenersatzrechts ist bei der Rechtswidrigkeit vor allem an eine unzureichende Sicherung der Daten oder überhaupt an eine unzulässige Erhebung von Daten ohne Einverständnis der Betroffenen zu denken. Das breite Spektrum von deliktischen Schadenersatzansprüchen kann sich aber auch beispielsweise auf das Auskunftsrecht des § 26 und vor allem auf die Richtigstellungspflicht des Auftraggebers nach § 27 stützen.

Für den Bereich des vertraglichen Schadenersatzes kommt vor allem eine vereinbarungswidrige Verarbeitung oder Weitergabe von Daten in Betracht, die jedoch zuvor rechtmäßig erfasst worden sind. Auch hier wird der

⁸⁷ Koziol, Haftpflichtrecht I³ Rz 4/90.

Richtigstellungspflicht des Auftraggebers nach § 27 große Bedeutung zukommen, zu denken ist an die Weitergabe von nicht mehr aktuellen Bonitätsdaten oder unrichtigen Patientendaten des Betroffenen, die ihm leicht einen größeren Schaden zufügen könnten.

4.6 Rechtswidrigkeitszusammenhang

Der Rechtswidrigkeitszusammenhang ist die Lehre vom Schutzzweck der Norm. Jemand soll für rechtswidrig zugefügte Schäden nur dann ersatzpflichtig werden, wenn die übertretene Norm den Eintritt gerade dieser Schäden verhindern soll. Bei einer Verschuldenshaftung wie der Schadenersatzpflicht ist also zu fragen, ob der Zweck des übertretenen Schutzgesetzes bzw der verletzten Vertragsklausel darin liegt, dass gerade der eingetretene Schaden verhindert werden soll. Es bedarf einer Auslegung im Einzelfall, wie weit der Rechtswidrigkeitszusammenhang reicht.⁸⁸

Aufgabe und somit Schutzzweck des DSG 2000 ist es, die unerlaubte Verwendung von personenbezogenen Daten zu verhindern, indem genau geregelt wird, in welchen Fällen die Daten von privaten und öffentlichen Auftraggebern ermittelt und verwendet werden dürfen. Auch werden die Betroffenen durch das in § 1 gewährte Grundrecht auf Datenschutz sowie durch die im fünften Abschnitt in den §§ 26 bis 28 normierten Rechte vor einer unerlaubten und unkontrollierten Weitergabe ihrer Daten und vor dem Bestehen inhaltlich inkorrektur Daten geschützt, indem die Rechte auf Auskunft, Richtigstellung, Löschung und Widerspruch eingeräumt werden.

Vom Schutzzweck des DSG 2000 sind sowohl die Daten selbst als auch jegliche Verwendung von personenbezogenen Daten in automationsunterstützter Form oder in manuellen Dateien umfasst. Da sowohl Auftraggeber des öffentlichen als auch des privaten Bereichs Adressaten der datenschutzrechtlichen Schutzpflichten sind, unterliegt jegliche Verwendung von personenbezogener Daten in oben beschriebener Form dem DSG 2000 und ist daher auch vom Schutzzweck der Norm umfasst. Anzumerken ist noch, dass der Gesetzgeber die

⁸⁸ *Koziol/Welser, Grundriss II*¹², 293ff.

Bestimmungen des DSG 2000 im Einzelfall auch als Schutzgesetz iSd § 1311 ABGB vorgesehen hat.⁸⁹

4.7 Verschulden

Während die Rechtswidrigkeit die objektiven Voraussetzungen für eine Überwälzung des Schadens umschreibt, regelt das Verschulden die subjektiven Voraussetzungen dafür. Wer ein Verhalten setzt, das er vermeiden hätte sollen oder vermeiden hätte können, handelt schuldhaft.⁹⁰ Es geht um die Frage, ob ein rechtswidriges Verhalten dem Täter auch vorwerfbar ist; allerdings muss das Verhalten vom Willen beherrschbar gewesen sein, da ansonsten keine Handlung im Rechtssinn vorliegt und sich die Frage nach dem Verschulden nicht mehr stellt.⁹¹ Mit dem Verschulden eng verbunden sind die Begriffe der Handlungs- bzw. Deliktsfähigkeit. Diese wird in § 153 iVm § 21 Abs 2 ABGB geregelt: Sie tritt mit dem Erreichen der Mündigkeit, also mit dem Vollenden des 14. Lebensjahres ein.

4.7.1 Vorsatz und Fahrlässigkeit

Die beiden Erscheinungsformen des Verschuldens sind der Vorsatz und die Fahrlässigkeit (§ 1294 ABGB spricht von „böser Absicht“ und „Versehen“). Vorsätzlich handelt, wem die Rechtswidrigkeit bewusst ist und wer gleichzeitig den schädlichen Erfolg vorhersieht und seinen Eintritt billigt.⁹² Fahrlässig handelt hingegen derjenige, der nicht maßstabsgerecht handelt und ein zumutbares rechtmäßiges Alternativverhalten, das nicht zum Eintritt des Schadens geführt hätte, nicht gesetzt hat.⁹³

Im Anwendungsbereich des DSG 2000 kommt sowohl vorsätzliches als auch fahrlässiges, zum Schadenersatz führendes Verhalten in Betracht. Auftraggeber, Dienstleister und deren Mitarbeiter haben gem § 15 das Datengeheimnis zu wahren und sind zu einer dem DSG 2000 entsprechenden Behandlung von personenbezogenen Daten verpflichtet. Wie bereits oben erwähnt sind nach dem Verbotsprinzip sämtliche zulässigen Verwendungsweisen von personenbezogenen Daten im DSG 2000 (zu der sowohl der Auftraggeber als

⁸⁹ ErläutRV 1613 BlgNR 20. GP 49.

⁹⁰ *Koziol/Welser*, Grundriss II¹², 299.

⁹¹ *Koziol*, Haftpflichtrecht I³ Rz 5/1.

⁹² *Koziol/Welser*, Grundriss II¹², 300.

⁹³ *Harrer in Schwimann*, ABGB VII² § 1297 Rz 11.

auch der Dienstleister angehalten sind) ausdrücklich normiert, jede dem DSG 2000 widersprechende Handlung bezüglich personenbezogener Daten ist schuldhaft iSd § 33 DSG 2000 und somit auch zumindest fahrlässig.

Vorsätzliches Handeln kommt beispielsweise in Betracht, wenn personenbezogene Daten gegen Entgelt ohne ausdrückliche Zustimmung des Betroffenen zur weiteren gewerbsmäßigen Nutzung weitergegeben und übermittelt werden (zB Adresslisten oder „schwarze Listen“ im Kreditauskunftsbereich).

An fahrlässiges Handeln ist etwa zu denken, wenn keine oder nur ungenügende Datensicherungsmaßnahmen iSd § 14 getroffen worden sind, zB wenn ein Firmennetzwerk nicht ausreichend vor dem Zugriff durch nicht berechtigte Dritte geschützt worden ist und sich ein Hacker personenbezogener Daten bemächtigt hat und beispielsweise durch erbeutete Kreditkartennummern den Betroffenen Schäden entstanden sind. Ein neuer Risikofaktor in Netzwerken sind drahtlose Funknetzwerke (WLANs) geworden, die im Empfangsbereich der Funksignale („hot spots“) verschiedene Computer miteinander vernetzen und so den Zugriff auf das gesamte Netzwerk (Intranet) ermöglichen. Leider sind solche Netzwerke oft falsch konfiguriert oder es wurde gänzlich auf Sicherungsmaßnahmen wie etwa die Verschlüsselung der Funkverbindung verzichtet, sodass es auch eigentlich nicht berechtigten Personen möglich ist, sich Zugriff auf das Netzwerk und somit auf darin gespeicherte Daten zu verschaffen. War der Netzwerkadministrator allzu sorglos, so genügt es uU sich mit einem WLAN-fähigen Notebook in die Nähe eines hot spots zu begeben, um völligen Zugriff auf ein Firmennetzwerk mit all seinen Kundendaten zu erlangen, ohne dass es auffällt oder gar verhindert werden kann. Eine derartige Sorglosigkeit im Umgang mit drahtlosen Netzwerken ist im Einzelfall eventuell sogar als grob fahrlässig einzustufen, zumindest leichte Fahrlässigkeit wird jedoch stets vorliegen, wenn auf diesem Wege Daten in falsche Hände geraten sind.

4.7.2 Beweislast

Grundsätzlich obliegt der Beweis des Verschuldens gem § 1296 ABGB dem Geschädigten – gelingt diesem der Beweis nicht, so hat er den Schaden selbst zu tragen. Wird jedoch eine vertragliche oder gesetzliche Verbindlichkeit oder eine

vertragsähnliche Schuld im Anbahnungsstadium eines Vertrages (culpa in contrahendo) verletzt, so kommt es nach § 1298 ABGB zu einer Beweislastumkehr: Nunmehr muss der Schädiger nachweisen, dass ihn kein Verschulden trifft.

In Umsetzung von Art 23 Abs 2 und Erwägungsgrund 55 der DS-RL enthält § 33 Abs 3 eine generelle Umkehr der Beweislast: Unabhängig vom Vorliegen einer vertraglichen oder vorvertraglichen Verbindlichkeit können sich sowohl der Auftraggeber als auch der Dienstleister von einer allfälligen Haftung befreien, wenn sie nachweisen, dass der den Schaden verursachende Umstand weder ihnen selbst noch ihren Leuten (vgl dazu die Ausführungen in Kapitel 4.8) zur Last gelegt werden kann – wenn der Schaden also entweder in gleicher Weise auch ohne Übertretung der Schutznorm eingetreten wäre oder aber (wenn entgangener Gewinn verlangt wird) nur leichte Fahrlässigkeit vorliegt.⁹⁴

Nicht der Geschädigte also hat ein Verschulden des Auftraggebers, des Dienstleisters oder deren Mitarbeitern zu beweisen, sondern der Auftraggeber oder der Dienstleister haben ihr Nicht-Verschulden nachzuweisen – diese Umkehr der Beweislast zugunsten des Betroffenen dient der Rechtssicherheit.⁹⁵

4.8 Gehilfenhaftung

Wie bereits oben erwähnt muss der Auftraggeber nicht notwendigerweise Daten selbst ermitteln oder verarbeiten, er kann sich auch eines Dienstleisters bedienen, der einzelne oder alle Verarbeitungsschritte für den Auftraggeber übernimmt. Sowohl Auftraggeber als auch Dienstleister können Aufträge in ihrem Zuständigkeitsbereich von Personen auf Dienst- oder Werkvertragsbasis erledigen lassen. Wie stellt sich nun die Situation dar, wenn eine solche (entweder vom Auftraggeber oder Dienstleister beauftragte) Person dem Betroffenen durch eine Fehlleistung einen Schaden zufügt?

Grundsätzlich ist festzustellen, dass sowohl einzelne, vom Auftraggeber oder vom Dienstleister beauftragte Personen als auch der Dienstleister selbst (durch die Beauftragung vom Auftraggeber) unter den Gehilfenbegriff fallen können. Das

⁹⁴ Dohr/Pollirer/Weiss, Datenschutzrecht², 228; Ghali, Datenschutz 397.

ABGB kennt zwei Arten von Gehilfen: Den Erfüllungsgehilfen (§ 1313a ABGB) und den Besorgungsgehilfen (§ 1315 ABGB).

Oft besteht zwischen dem Geschädigten und dem Auftraggeber kein Vertragsverhältnis, sodass die Erfüllungsgehilfenregelung des § 1313a ABGB (Haftung für Erfüllungsgehilfen wie für eigenes Verschulden) nicht zur Anwendung käme und der Auftraggeber nur gem § 1315 ABGB für eine untüchtige oder wissentlich gefährliche Person, der er sich bedient hat, haften müsste (Besorgungsgehilfenhaftung). In der Praxis hat sich jedoch herausgestellt, dass es oft für den geschädigten Betroffenen unmöglich ist einen genauen Einblick in die Arbeitsaufteilung zwischen Auftraggeber, Dienstleister und deren Arbeitnehmer bei einer Verarbeitung von personenbezogenen Daten zu gewinnen und somit die Verantwortlichkeit der handelnden Personen festzustellen.⁹⁶ Der Gesetzgeber hat sich aus diesem Grund dazu entschlossen in Gestalt des § 33 Abs 2 DSG 2000 die Erfüllungsgehilfenhaftung des § 1313a ABGB auch auf jene Fälle auszudehnen, in denen keine vertragliche Beziehung zwischen Geschädigtem und Auftraggeber vorliegt: Dem Auftraggeber und dem Dienstleister werden sämtliche Fehlleistungen der von ihnen beauftragten Personen zugerechnet, wobei im Falle eines Fehlverhaltens des Dienstleisters dieser ein Gehilfe des Auftraggebers ist. Die Haftung des Auftraggebers gegenüber dem Geschädigten ist somit nicht mehr nur auf die bloße Besorgungsgehilfenhaftung reduziert, sondern es kommt sinngemäß zu einer Haftung analog zu § 1313a ABGB: Auftraggeber (und Dienstleister) haften für jegliche Fehlleistungen ihrer Leute wie für das eigene Verschulden. Der Begriff „Leute“ des § 33 Abs 2 umfasst somit sowohl die vom Auftraggeber und Dienstleister zur Erbringung einer Leistung bei der Verarbeitung von Daten beauftragten Personen als auch den Dienstleister als Gehilfen des Auftraggebers selbst – die Haftung gegenüber dem Betroffenen soll zunächst beim Auftraggeber konzentriert werden.⁹⁷

Hinsichtlich etwaiger Regressansprüche des Geschäftsherrn gegenüber seinem Gehilfen schweigt das DSG 2000, es finden daher im privaten Bereich die allgemeinen Bestimmungen des bürgerlichen Rechts Anwendung. Nach § 1313

⁹⁵ *Drobesch/Grosinger*, Datenschutzgesetz 245.

⁹⁶ ErläutRV 1613 BlgNR 20. GP 49.

⁹⁷ *Ghali*, Datenschutz 196.

ABGB kann der Geschäftsherr Rückersatzansprüche gegenüber seinem Gehilfen geltend machen, die im Anwendungsbereich des DHG jedoch stark eingeschränkt werden: Gem § 2 Abs 3 DHG haftet der Arbeitnehmer seinem Arbeitgeber nicht für entschuldbare Fehlleistungen, bei leichter Fahrlässigkeit kann ihn der Richter aus Gründen der Billigkeit von der Ersatzpflicht gänzlich befreien und bei grober Fahrlässigkeit besteht ein richterliches Mäßigungsrecht (§ 2 Abs 1 DHG) – nur bei vorsätzlichem Handeln des Arbeitnehmers besteht keine Haftungserleichterung.

4.9 Mitverantwortung des Geschädigten

Ein Aspekt des Schadenersatzrechts ist die Mitverantwortung des Geschädigten. Nicht immer liegt ein reines Fremdverschulden vor, oft hat auch der Geschädigte selbst durch eigenes Fehlverhalten zur Entstehung des Schadens beigetragen. Im Datenschutzbereich ist hierbei vor allem an das allzu sorglose Ausfüllen von diversen Fragebögen in Verbindung mit diversen Gewinnspielen und Preisausschreiben und die (meist unzulässige) Weitergabe dieser Daten zu denken. Auch kommt es im Computerbereich oft vor, dass sorglose Benutzer sämtliche relevanten Daten wie beispielsweise Passwörter und andere Zugriffsberechtigungen in einer einzigen, noch dazu aufgrund des Dateinamens und des Speicherortes leicht zu identifizierbaren Datei speichern und sich im Anschluss über diesen Computer ins Internet verbinden, ohne den Computer vorher entsprechend gesichert zu haben (wie zB durch die Verwendung einer Firewall). In diesen Fällen ist es Hackern oft ein Leichtes, sich Zugang zum jeweiligen System zu verschaffen und sich auch der persönlichen Daten des Benützers zu bemächtigen.

Durch das Verbotsprinzip ist eine Verwendung von personenbezogenen Daten nur in den ausdrücklich normierten Fällen für zulässig erklärt worden. Im Wesentlichen muss der Betroffene zu allen relevanten Verwendungs- und Verarbeitungsschritten seine Zustimmung geben; somit ist die Zahl der möglichen Fälle einer Mitverantwortung des geschädigten Betroffenen erheblich reduziert worden. Haben der Betroffene oder eine Person, deren Verhalten er zu vertreten hat (dies kann zB ein Dienstnehmer des Betroffenen sein) dennoch durch eigenes Fehlverhalten zum Eintritt des Schadens beigetragen, so verweist § 33 Abs 3 letzter Satz auf die allgemeine Regelung des § 1304 ABGB: Dem Betroffenen

gebührt in diesem Fall nicht der volle Ersatz seines Schadens, sondern der auf sein Mitverschulden entfallende Anteil des Schadens wird prozentuell vom Gesamtschaden abgezogen und muss selbst getragen werden. Lässt sich das Mitverschulden nicht feststellen, so wird der Schaden im Zweifel zu gleichen Teilen zwischen Schädiger und geschädigtem Betroffenen aufgeteilt.

In der Praxis wird im Falle eines behaupteten Mitverschuldens entweder von Amts wegen oder auf Antrag einer Partei vorerst mit Zwischenurteil über den Grund des Anspruchs sowie (bei bewiesenem Mitverschulden) über die verhältnismäßige Teilung entschieden. Erst nach Eintritt der Rechtskraft des Zwischenurteils entscheidet das Gericht über die Höhe des Anspruchs mit Endurteil, um in Verfahren mit hohen Sachverständigenkosten wie etwa bei der Feststellung von entgangenem Gewinn nicht bereits vor der Entscheidung der letzten Instanz (die das Klagebegehren eventuell zur Gänze abweist) hohe Prozesskosten zu verursachen.⁹⁸

4.10 Immaterieller Schadenersatz

Anders als nach dem DSG 1978 kann ein Betroffener nunmehr bei Vorliegen der Voraussetzungen des § 33 Abs 1 auch immateriellen Schadenersatz als Ausgleich für die Bloßstellung in der Öffentlichkeit geltend machen, das DSG 2000 verweist in seinem § 33 Abs 1 zweiter Satz auf das MedG. In dessen § 7 wird der Medieninhaber bei einer Verletzung des höchstpersönlichen Lebensbereiches einer Person, die sie in der Öffentlichkeit bloßstellt, zu einer Entschädigung für den erlittenen Schaden angehalten. Datenschutzrechtlich handelt es sich dabei um Fälle schwerwiegender und rechtswidriger Datenverwendungen. Die Qualität der Bloßstellung nach § 33 Abs 1 DSG 2000 kommt dabei jener nach § 7 MedG gleich und nach dem Willen des Gesetzgebers sollen die gleichen Höchstgrenzen für den Entschädigungsbetrag gelten, der Bereich des Medieninhaltsdeliktes des § 7 MedG sollte jedoch nicht ausgeweitet werden.⁹⁹

⁹⁸ Ghali, Datenschutz 397f.

⁹⁹ Drobesch/Grosinger, Datenschutzgesetz 245.

Bedingung für einen Ersatz immaterieller Schäden nach § 33 Abs 1 DSG 2000 iVm § 7 Abs 1 MedG ist das (kumulative) Vorliegen folgender Voraussetzungen, auf die im Folgenden näher eingegangen wird:

- Rechtswidrige und öffentlich zugängliche Verwendung von
 - sensiblen Daten oder
 - strafrechtlich relevanten Daten iSd § 8 Abs 4 DSG 2000 oder
 - Daten über die Kreditwürdigkeit des Betroffenen
- Verletzung des höchstpersönlichen Lebensbereiches
- Bloßstellung in der Öffentlichkeit

4.10.1 Rechtswidrige oder öffentlich zugängliche Verwendung

Auch wenn die DSG 2000-widrige Verwendung der in § 18 Abs 2 Z 1 bis 3 angeführten Datenarten nicht ausdrücklich in § 33 Abs 1 S 2 genannt ist, so ergibt sich aus der RV, dass der Gesetzgeber neben einer fehlerhaften auch eine rechtsmissbräuchliche Datenverwendung mitumfasst haben wollte¹⁰⁰ und demnach auch eine rechtswidrige Verwendung von Daten Regelungsgegenstand des § 33 Abs 1 zweiter Satz ist.

Eine öffentliche Zugänglichkeit von Daten liegt immer dann vor, wenn jedermann unter den gleichen Voraussetzungen Einsicht in diese Daten nehmen und davon Kenntnis erlangen kann. Dies kann durch Veröffentlichung der Daten in Medien geschehen, aber auch beispielsweise durch Erweiterung öffentlicher Telefonbücher durch den Zusatz „ethnische Herkunft“ oder durch das Aufnehmen von Daten über die Kreditwürdigkeit in öffentlich zugängliche Kundenlisten.

4.10.2 Die Datenarten des § 18 Abs 2 Z 1 bis 3

Nicht jegliche Verwendung von Daten, die zu einer Bloßstellung iSd § 7 Abs 1 MedG führt, berechtigt zum (immateriellen) Schadenersatz – die erlittene Kränkung muss durch die Verwendung von bestimmten (der Vorabkontrolle unterliegenden) Datenarten, die in § 18 Abs 2 Z 1 bis 3 DSG 2000 angeführt sind, verursacht worden sein.

¹⁰⁰ ErläutRV 1613 BlgNR 20. GP 49.

Es handelt sich dabei um folgende Kategorien von Daten:

- Z 1: Sensible Daten. Näheres zu dieser Datenart in Kapitel 3.1.1.3.
- Z 2: Strafrechtlich relevante Daten iSd § 8 Abs 4. Es handelt sich dabei um Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen. Erfasst sind weiters auch Daten, die den Verdacht der Begehung von Straftaten, strafrechtliche Verurteilungen oder vorbeugende Maßnahmen iSd §§ 21 bis 23 StGB zum Inhalt haben. Es handelt sich dabei nicht um sensible Daten, Art 8 Abs 5 DS-RL rückt sie jedoch in die Nähe dieser Daten. Zu beachten ist, dass nicht nur Daten über Verurteilte selbst, sondern auch Daten über Angeklagte, Beschuldigte oder bloße Tatverdächtige vom Schutz des § 8 Abs 4 umfasst sind.¹⁰¹
- Z 3: Daten, die die Auskunftserteilung über die Kreditwürdigkeit des Betroffenen zum Inhalt haben. Hier ist vor allem in Hinblick auf eine öffentliche Bloßstellung des Betroffenen an die Veröffentlichung von „schwarzen (Branchen)Listen“ zu denken – es soll in der Privatsphäre des Einzelnen bleiben, ob und warum beispielsweise die Hausbank einen Kredit verweigert hat um den Betroffenen nicht etwa gegenüber den Nachbarn bloßzustellen. Auch ist zu beachten, dass eine publik gemachte Nicht-Kreditwürdigkeit dem Betroffenen auch im Berufsleben erheblich zur Last fallen kann, da sich beispielsweise Arbeitgeber in der Regel wohl lieber kreditwürdige Arbeitnehmer suchen werden.

4.10.3 Verletzung des höchstpersönlichen Lebensbereichs

Das Gut, das durch § 7 MedG geschützt wird, ist der höchstpersönliche Lebensbereich einer Person. Dieser höchstpersönliche Lebensbereich wird nirgendwo im MedG definiert, sondern muss den Materialien zum MedG entnommen werden: Demnach sind vor allem das Leben in der Familie, die Gesundheitssphäre und das Sexualleben zum höchstpersönlichen Lebensbereich einer Person zu zählen. Der Gesetzgeber hat zudem noch eine inhaltliche Deckung des Begriffes des höchstpersönlichen Lebensbereiches mit dem des Privat- und Familienlebens iSd Art 8 MRK vorgesehen.¹⁰² Vermögensverhältnisse, Unternehmensbeteiligungen oder Angelegenheiten des Geschäfts- oder

¹⁰¹ *Drobesch/Grosinger*, Datenschutzgesetz 140.

¹⁰² JAB 743 BlgNR 15. GP 6.

Berufslebens wie etwa das Einkommen, der Vermögensstand oder die berufliche Tätigkeit werden jedoch nicht unter diesem Begriff subsumiert. Die Schutzgüter des § 7 MedG sind demnach die Privatsphäre¹⁰³ sowie der Schutz der Entfaltung der Person und der Menschenwürde an sich.¹⁰⁴ Geschützt wird aber nicht das gesamte Privatleben einer Person, sondern eben nur der „höchst“-persönliche Lebensraum. Eine Abgrenzung, wann eine Angelegenheit nur mehr „persönlich“ ist und somit nicht mehr vom Schutz des § 7 umfasst ist, fällt in der Praxis schwer, die Abwägungsklausel entspricht jedenfalls dem Erforderlichkeits- und Verhältnismäßigkeitsprinzip des Art 10 Abs 2 MRK.¹⁰⁵ Geschützt wird die Intimsphäre einer Person, zu der sowohl körperliche (zB Krankengeschichte oder körperliche Defekte) als auch geistige Merkmale (wie Geisteskrankheiten, der Intelligenzquotient oder die Ergebnisse von psychologischen Tests) zählen. Nach der Rechtsprechung fallen sowohl häusliche Auseinandersetzungen mit dem Ehepartner¹⁰⁶, (festgestellt im Prozess einer früheren Prostituierten Jack Unterwegers gegen „News“ im Zuge der Kriminalberichterstattung desselben Blattes) die frühere Ausübung von Prostitution (nicht jedoch die gegenwärtige, öffentlich ausgeübte Prostitution)¹⁰⁷ oder aber auch die Veröffentlichung von Nacktfotos, noch dazu auf der Titelseite einer Zeitschrift¹⁰⁸ unter den Begriff des höchstpersönlichen Lebensbereichs. Auch Berichte über privates Handeln in öffentlichen Räumen (Gegebenheiten der so genannten „Privatöffentlichkeit“) sind von § 7 geschützt, um den Einzelnen die Entfaltung seines Privatlebens in öffentlichen Räumen (wie beispielsweise der Besuch von Veranstaltungen) auch ohne Anteilnahme der Massenmedien zu ermöglichen;¹⁰⁹ es muss sich jedoch um Informationen handeln, die besonders schutzwürdig im Hinblick auf die Privatsphäre sind. Vom höchstpersönlichen Lebensbereich des § 7 nicht mehr umschlossen sind Verhaltensweisen mit starkem sozialen Bezug oder ein an die Öffentlichkeit gerichtetes Verhalten wie die oben erwähnte öffentlich ausgeübte Prostitution oder aber auch der Umstand, dass jemand eine Straftat begangen hat bzw einer solchen verdächtigt wird (ein neuerliches Aufgreifen einer schon weiter zurückliegenden Straftat nach Verurteilung und Verbüßung der Strafe greift

¹⁰³ Berka in *Berka/Höhne/Noll/Polley*, Mediengesetz Praxiskommentar (2002) § 7 Rz 7.

¹⁰⁴ *Brandstetter/Schmid*, Kommentar zum Mediengesetz² (1999) § 7 Rz 1.

¹⁰⁵ *Foregger/Litzka*, Mediengesetz⁴ (2000) 55.

¹⁰⁶ OLG Wien 18 Bs 272/98, MR 1999, 68.

¹⁰⁷ OLG Wien 18 Bs 28/95, MR 1997, 17.

¹⁰⁸ OGH 4 Ob 2249/96f, *ecolex* 1997, 34 = MR 1997, 28 = ÖBl 1997, 140.

allerdings wieder in die Privatsphäre ein¹¹⁰ und wird im Falle des Vorwerfens zudem auch noch nach § 113 StGB mit Strafe bedroht).

4.10.4 Bloßstellung in der Öffentlichkeit

Wurde der höchstpersönliche Lebensbereich einer Person durch eine Veröffentlichung berührt, so kommt es dennoch nicht schon aus diesem Grund alleine zum Schadenersatz: Es muss zusätzlich noch zu einer Bloßstellung des Betroffenen in Form von Erörterungen (in schriftlicher Form) oder Darstellungen (bildhafte Berichterstattung wie beispielsweise Fotos) in der Öffentlichkeit gekommen sein. Der mit der Bloßstellung verbundene Verletzungstatbestand kann mit dem „medialen Eindringen in eine schutzwürdige Privatsphäre und die damit verbundene Beschädigung der persönlichen Integrität“¹¹¹ umschrieben werden; dabei handelt es sich um die Preisgabe von „intimsten Angelegenheiten, die manchmal ängstlich als Geheimnis gehütet werden.“¹¹² Es kommt einzig und allein auf eine Bloßstellung an, nicht hingegen auf die Gefahr einer Rufschädigung oder einer Minderung des Ansehens – dabei ist stets ein objektiver Maßstab anzulegen und die persönlichen Eigenheiten des Betroffenen (wie etwa eine übertriebene Empfindlichkeit oder aber im umgekehrten Fall eine besonders „dicke Haut“) sind außer Acht zu lassen; es kommt darauf an, ob eine andere Person in der gleichen Situation ähnlich empfunden hätte. Der Nachweis einer nachteiligen Wirkung der Bloßstellung für den Betroffenen ist nicht notwendig, da es einzig und allein auf die Indiskretion und den damit verbundenen Eingriff in die Persönlichkeitsrechte ankommt. Positive Nachrichten können nicht bloßstellend wirken, da eine Bloßstellung stets eine negative Voreingenommenheit der Öffentlichkeit schafft.¹¹³ Uneinig ist sich die Lehre, ob bereits bekannte Tatsachen zu einer Bloßstellung führen können: *Berka*¹¹⁴ bejaht dies, anderer Ansicht sind *Brandstetter/Schmid*.¹¹⁵ Bei wissenschaftlichen oder künstlerischen Werken können jedenfalls Eingriffe in den höchstpersönlichen Lebensbereich durch die Kunst- und Wissenschaftsfreiheit (Art 17 und 17a StGG) auch dann zulässig sein, wenn sie andernfalls ohne diese Grundrechte nicht mehr erlaubt wären. Allerdings darf die

¹⁰⁹ *Berka* in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 10.

¹¹⁰ OLG Wien 27 Bs 27/86, MR 1986/5, 9.

¹¹¹ *Berka* in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 17.

¹¹² *Brandstetter/Schmid*, Kommentar² § 7 Rz 8.

¹¹³ *Brandstetter/Schmid*, Kommentar² § 7 Rz 12.

¹¹⁴ *Berka* in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 19.

damit verbundene Bloßstellung nicht den wissenschaftlichen oder künstlerischen Rahmen sprengen. Die von § 7 MedG geforderte öffentliche Bloßstellung durch ein Medium iSd § 1 Abs Z 1 kann jedenfalls entfallen, da § 33 Abs 1 DSG 2000 eine Ersatzpflicht für die erlittene Kränkung ausdrücklich auch für jene Fälle vorsieht, in denen die Bloßstellung nicht in einem Medium geschieht.

In § 7 Abs 2 sind vier Ausnahmetatbestände normiert, die eine an sich bloßstellende und zum Schadenersatz führende Berichterstattung dennoch zulässig machen:

Bei Z 1 handelt es sich um eine Konkretisierung der in Art 33 und Art 96 B-VG verfassungsmäßig gewährleisteten Rechte: Wahrheitsgetreue Berichte über öffentliche Sitzungen der allgemeinen Vertretungskörper oder einen ihrer Ausschüsse (nicht aber über Sitzungen des Gemeinderates, der rechtlich nur ein Verwaltungsorgan ist) haben keine Entschädigungsfolgen.

Der Entschädigungsanspruch ist gem Z 2 auch dann ausgeschlossen, wenn die Veröffentlichung einerseits wahr ist und andererseits im Zusammenhang mit dem öffentlichen Leben steht, da hier die öffentlichen Informationsinteressen vorgehen. Im Zweifelsfall hat der Medieninhaber (vgl § 1 Abs 1 Z 8) den Wahrheitsbeweis anzutreten; scheitert er, so führt dies wiederum zu Entschädigungsansprüchen nach § 7. Das „öffentliche Leben“ ist der Bereich des öffentlichen Handelns in gemeinschaftswichtigen Angelegenheiten, an dem ein besonderes Informationsinteresse der Öffentlichkeit besteht; es wird auf den Lebenskreis und auf einen Zusammenhang mit der öffentlichen Funktion des Betroffenen abgestellt.¹¹⁶ Davon umfasst ist einerseits der staatliche Bereich, der das politische Leben und die Tätigkeit der Organwalter in den drei staatlichen Gewalten Gesetzgebung, Verwaltung und Gerichtsbarkeit einschließt und andererseits der nicht-staatliche Bereich wie etwa Kunst oder Sport. *Brandstetter/Schmid*¹¹⁷ bejahen die Zugehörigkeit von Stars des Showgeschäfts zum öffentlichen Leben (dies verneint jedoch *Berka*¹¹⁸). Erlaubt und zulässig sind

¹¹⁵ *Brandstetter/Schmid*, Kommentar² § 7 Rz 10.

¹¹⁶ *Brandstetter/Schmid*, Kommentar² § 7 Rz 20.

¹¹⁷ *Brandstetter/Schmid*, Kommentar² § 7 Rz 21.

¹¹⁸ *Berka* in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 26.

demnach etwa Berichte über den Gesundheitszustand des Bundespräsidenten, der die Bevölkerung interessieren darf, fraglich wäre eine mediale Berichterstattung über die Seitensprünge eines Fußballstars, der als Person des öffentlichen Lebens trotzdem ein Recht auf die Respektierung seines höchstpersönlichen Lebensraumes hat – hier müsste wohl im Einzelfall abgewogen werden, ob die Berichterstattung adäquat ist oder nicht.

Eine Einwilligung des Betroffenen schließt gem Z 3 Ersatzansprüche ebenfalls aus. Dabei ist zu beachten, dass nicht nur eine ausdrückliche, sondern auch eine konkludente Zustimmung erteilt werden kann. Denkbar ist eine (wenn nicht konkludent gegebene) Zustimmung weiters auch dann, wenn diese aus den Umständen angenommen werden konnte, beispielsweise wenn der Betroffene Details aus seinem Privatleben selbst öffentlich gemacht hat und die Berichterstattung sich darauf bezieht.¹¹⁹ Es ist aber darauf Bedacht zu nehmen, dass eine vermutete Zustimmung nicht fingiert werden darf und stets auf den konkreten Anlass bezogen werden muss.

Der letzte Ausnahmetatbestand, der einen Eingriff in den höchstpersönlichen Lebensbereich eines Betroffenen zulässig macht, ist schließlich der Umstand, dass es sich gem Z 4 um eine Live-Sendung im Rundfunk handelt (Fernsehen, Radio und wohl auch Live-Streams im Internet), bei der kein Mitarbeiter oder Auftraggeber die gebotene journalistische Sorgfalt außer Acht gelassen hat. Diese Personen werden im Zuge der Sendung darauf hinwirken müssen, dass vermeidbare Enthüllungen unterbleiben.¹²⁰

Denkbare Konstellationen, die zu einem Anspruch auf immateriellen Schadenersatz nach § 33 Abs 1 DSGVO 2000 iVm § 7 Abs 1 MedG führen könnten, wären etwa die Zurverfügungstellung von öffentlichen Namenslisten, die auch Daten über die Kreditwürdigkeit der angeführten Personen verbunden mit zynischen Kommentaren enthalten, die Führung eines öffentlichen Registers (etwa im Internet), welches sämtliche Vorstrafen der gesamten Nachbarschaft enthält und als „Pranger“ wirkt (was in den USA teilweise bereits Realität ist) oder aber

¹¹⁹ Berka in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 29.

¹²⁰ Berka in *Berka/Höhne/Noll/Polley*, Mediengesetz § 7 Rz 31.

das Vorwerfen einer (erwiesenermaßen zugezogenen) Geschlechtskrankheit und deren Zurückführung dessen auf einen „untugendhaften“ Lebensstil.

4.10.5 Geltendmachung und Bemessung der Entschädigung

Verstöße gegen § 7 MedG, die auch nicht durch einen der Ausnahmetatbestände des Abs 2 für zulässig erklärt werden, berechtigen zu einer Entschädigung für die erlittene Kränkung, also zu immateriellen Schadenersatz. Dieser ist nach § 33 Abs letzter Satz DSG 2000 gegenüber dem Auftraggeber der Datenverwendung geltend zu machen. Gem § 7 Abs 1 MedG darf der Entschädigungsbetrag 14.535 € nicht übersteigen; hinsichtlich der Bemessung wird auf § 6 Abs 1 zweiter Satz verwiesen: Demnach ist bei der Festlegung der Höhe des Entschädigungsbetrages durch den Richter auf den Umfang und die Auswirkungen sowie auf die Art der Verbreitung der Veröffentlichung (wie bereits erwähnt kann gem § 33 Abs 1 S 2 DSG 2000 eine Entschädigung auch zugesprochen werden, wenn die öffentlich zugängliche Verwendung von personenbezogenen Daten nicht in Form eines Mediums iSd § 1 Abs 1 Z 1 MedG erfolgt) Bedacht zu nehmen, nach freiem richterlichem Ermessen vorzugehen und ein Pauschalbetrag zuzusprechen. Dem Kläger wird das Verfahren erleichtert: Einerseits gibt es kein Beweisverfahren über die Höhe der Entschädigung, andererseits muss der Kläger sein Begehren nur auf eine „angemessene Entschädigung“ richten und geht somit kein Kostenrisiko im Falle der Abweisung des Mehrbetrages ein.¹²¹

Es stellt sich jedoch die Frage, ob im Wege einer teleologischen Interpretation die Regelung des § 6 Abs 1 zweiter Satz 2. HS, nämlich dass im Falle eines Zuspruchs eines Entschädigungsbetrages auf die Wahrung der wirtschaftlichen Existenz des Medienunternehmers (§ 1 Abs 1 Z 6) Rücksicht zu nehmen ist, sinngemäß statt dessen auf den Auftraggeber, gegen den der Entschädigungsanspruch geltend gemacht wird, angewendet werden soll. Gegen diese Auslegungsvariante spricht jedenfalls die Wortinterpretation: § 33 Abs 1 letzter Satz DSG 2000 bestimmt, dass (entgegen der Bestimmung des § 7 Abs 1 MedG) nicht der Medieninhaber, sondern der Auftraggeber der Datenverarbeitung zum Schadenersatz verpflichtet wird; § 6 Abs 1 S 2 2. HS bezieht sich nur auf das Medienunternehmen und § 33 DSG 2000 stellt (im Gegensatz zur Frage, gegen

¹²¹ *Dohr/Pollirer/Weiss, Datenschutzrecht², 228.*

wen der Schadenersatzanspruch geltend zu machen ist) nicht ausdrücklich klar, dass zudem eben auch auf die wirtschaftliche Existenz des datenschutzrechtlichen Auftraggebers Bedacht zu nehmen ist. Im Umkehrschluss könnte man zu der Ansicht gelangen, dass es sich um ein bewusstes Schweigen des Gesetzgebers handelt und der 2. HS des § 6 Abs 1 S 2 MedG keine Anwendung bei Schadenersatzansprüchen nach § 33 Abs 1 DSG 2000 iVm § 7 Abs 1 MedG finden soll.

Richtiger erscheint aber die Ansicht, analog zur Regelung zugunsten des Medienunternehmens ebenso auf die wirtschaftliche Existenz des Auftraggebers einer Datenanwendung Rücksicht zu nehmen, da es unsachlich erscheint zwar auf den Medienunternehmer, nicht jedoch auf den datenschutzrechtlichen Auftraggeber Bedacht zu nehmen, denn auch dieser kann im Falle einer Verurteilung zu Schadenersatz in seiner wirtschaftlichen Existenz gefährdet werden. Zwar könnte man meinen, dass die öffentlich zugängliche Verwendung von personenbezogenen Daten schwerer wiegt als eine Bloßstellung nach dem MedG, jedoch erscheint es dennoch zweckmäßig auf die wirtschaftliche Existenz von va kleineren Auftraggebern Rücksicht zu nehmen.

4.10.6 Zusammentreffen von mehreren Ansprüchen

Das Verhältnis von Schadenersatzansprüchen nach § 33 DSG 2000 und solchen nach § 7 MedG ist vom Gesetzgeber nicht ausdrücklich normiert worden. *Drobesch/Grosinger*¹²² interpretieren die ErläutRV dahingehend, dass beide Ansprüche unabhängig voneinander geltend gemacht werden können und es somit zu einem bewussten Nebeneinander beider Ansprüche kommen kann, deren Verhältnis ähnlich zu sehen ist, wie die Ansprüche nach § 78 UrhG und § 7 MedG (jeweils getrennte Geltendmachung unabhängig voneinander).¹²³

4.11 Verfahrensrecht

4.11.1 Zuständigkeit

Ansprüche des Betroffenen wegen Verletzung des Rechts auf Geheimhaltung, Richtigstellung oder Löschung, die sich gegen einen Auftraggeber des privaten Bereichs richten, sind nicht vor der DSK geltend zu machen, sondern gem § 1 Abs

¹²² *Drobesch/Grosinger*, Datenschutzgesetz 245.

5 iVm § 32 Abs 1 auf dem Zivilrechtsweg. Für Schadenersatzansprüche, deren Ursache in einer dem DSG 2000 zuwideren Handlung liegt, hat der Gesetzgeber ebenfalls den Gang vor die ordentlichen Gerichte vorgesehen, indem § 33 Abs 4 auf § 32 Abs 4 verweist. Demnach ist in 1. Instanz sachlich das Landesgericht zuständig, die örtliche Zuständigkeit richtet sich entweder nach dem gewöhnlichen Aufenthalt oder Sitz des Betroffenen oder aber auch wahlweise nach dem gewöhnlichen Aufenthalt oder Sitz des Auftraggebers oder des Dienstleisters. Die örtliche Zuständigkeit für Streitigkeiten zwischen dem Auftraggeber und seinem Dienstleister sowie zwischen dem Dienstleister und seinem Sub-Dienstleister richtet sich nach den allgemeinen Regeln der §§ 65ff JN. *Dohr/Pollirer/Weiss*¹²⁴ weisen zudem auch noch auf die Vorteilhaftigkeit von Schiedsgerichten hinsichtlich der Raschheit, der Sachkenntnis der Richter, der Kosten und der Vergleichsmöglichkeit hin.

4.11.2 Nebenintervention der DSK

Die DSK kann auf Verlangen des Betroffenen und zur Wahrung von geschützten Interessen einer größeren Anzahl von Betroffenen gem § 32 Abs 6 DSG 2000 dem Prozess auf Seiten des Betroffenen zur Unterstützung als Nebenintervenient (§§ 17ff ZPO) beitreten. Aufgrund der individuellen Natur von Schadenersatzansprüchen nach § 33 sind diese (anders als Feststellungsansprüche) jedoch nicht für die datenschutzrechtlichen Interessen einer größeren Zahl von Betroffenen relevant und können somit nicht Gegenstand einer Nebenintervention durch die DSK nach § 32 Abs 6 sein.¹²⁵

4.11.3 Verjährung

Hinsichtlich der Verjährung von Schadenersatzansprüchen ist zunächst festzustellen, dass § 33 Abs 4 auf § 32 Abs 4 verweist. Für Klagen nach § 32 bestimmt § 34 Abs 1 eine Verjährungsfrist von einem bzw drei Jahren, da eine Ermittlung von Sachverhalten, die schon lange zurückliegen, oft Schwierigkeiten bereitet und eine verlässliche Beurteilung, ob nun eine Datenschutzverletzung vorlag oder nicht, verhindert wird. Hinsichtlich der Geltendmachung von Schadenersatzansprüchen nach § 33 stellen die ErläutRV jedoch ausdrücklich

¹²³ OLG Wien 1 R 6/97, MR 1997, 76.

¹²⁴ *Dohr/Pollirer/Weiss*, Datenschutzrecht², 230ff.

¹²⁵ DSK 1.6.2001, K073.020/006-DSK/2001, RIS.

klar, dass trotz der Verweisung auf § 32 Abs 4 für Ansprüche nach § 33 die kurzen Verjährungsfristen des § 34 Abs 1 keine Geltung haben. In Ermangelung spezieller Regelungen gelten diesbezüglich die Verjährungsfristen des § 1489 ABGB:¹²⁶ Die (relative) Verjährungsfrist beträgt drei Jahre gerechnet ab dem Zeitpunkt der Kenntnis von Schaden und Schädiger - ist dem Betroffenen entweder der Schaden oder die Person des Schädigers unbekannt oder ist der Schaden aus einer oder mehreren gerichtlich strafbaren Handlungen, die nur vorsätzlich begangen werden können und mit mehr als einjähriger Freiheitsstrafe bedroht sind, entsprungen (somit kommt das Delikt der Sachbeschädigung nach § 125 StGB nicht in Betracht, wohl aber das Delikt der Datenbeschädigung nach § 126a StGB in der Qualifikation des Abs 2), so beträgt die (absolute) Verjährungsfrist dreißig Jahre.

Zu beachten bleibt jedoch, dass in Fällen der Anwendung des Rechts anderer Mitgliedstaaten im Inland gem § 3 DSG 2000 bezüglich Unterlassungs-, Lösungs-, Richtigstellungs- und auch Schadenersatzansprüchen die Verjährungsvorschriften dieser Mitgliedsstaaten zur Anwendung kommen.¹²⁷

5. Kritische Gedanken zu § 33 DSG 2000

Wie eingangs erwähnt ist das österreichische DSG 2000 eine Konsequenz des Europarechts, namentlich der DS-RL, die in nationales Recht transformiert werden musste. Es stellt sich bezüglich mehrerer Punkte die Frage, ob der österreichische Gesetzgeber alle Vorgaben des Gemeinschaftsrechts korrekt erfüllt hat und des weiteren ist kritisch zu hinterfragen, ob aus der Formulierung des § 33 tatsächlich das Optimum herausgeholt worden ist, sprich ob diese Norm klar und verständlich gefasst ist und keinerlei Unklarheiten aufwirft.

Einerseits musste sich der Gesetzgeber für die verspätete Umsetzung in das nationale Recht Kritik gefallen lassen (die 3-jährige Umsetzungsfrist nach Art 32 Abs 1 DS-RL lief am 24.10.1998 ab, das DSG 2000 trat jedoch erst am 1.1.2000

¹²⁶ ErläutRV 1613 BlgNR 20. GP 50.

¹²⁷ *Kilches*, Datenschutzgesetz 2000 – Selbstbestimmter Datenschutz, MR 1999, 261 (267 FN 30).

in Kraft), andererseits stellt sich die Frage, ob die Schadenersatzregelung des Art 23 DS-RL in Gestalt des § 33 DSG 2000 korrekt umgesetzt worden ist. Ist die DS-RL nicht korrekt ins österreichische Recht umgesetzt worden, so kommt es selbst bei einer inhaltlich ausreichenden Bestimmtheit der DS-RL zu keiner unmittelbaren Anwendbarkeit der RL im Verhältnis zwischen Privaten untereinander (und das ist für den Anwendungsbereich des § 33 DSG 2000 der Fall, weil als grundlegende Voraussetzung der Auftraggeber dem privaten Bereich zugerechnet werden muss), da der EuGH eine horizontale Drittwirkung von RL ausdrücklich abgelehnt hat.¹²⁸ Die DS-RL wäre für den nationalen Rechtsanwender jedoch insofern dennoch von Bedeutung, als das nationale Gericht zur richtlinienkonformen Interpretation des § 33 DSG 2000 verpflichtet wäre.

5.1 Verschuldensunabhängige Haftung?

Ein Standpunkt in der Lehre¹²⁹ meint, dass eine schadenersatzrechtliche Haftung nach Art 23 DS-RL unabhängig vom Verschulden sei und somit ein solches nicht voraussetze (ohne dies jedoch zu begründen). Nach dieser Ansicht käme es zu einer Gefährdungshaftung. Träfe dies zu, so stünde § 33 DSG 2000 im Widerspruch zum Gemeinschaftsrecht, da in dessen Abs 1 von einer „schuldhaften“ Verwendung von personenbezogenen Daten entgegen den Bestimmungen des DSG 2000 die Rede ist und auf die allgemeinen Bestimmungen des bürgerlichen Rechts verwiesen wird, wonach es jedenfalls zu einer Verschuldenshaftung kommen soll; insofern wäre die DS-RL unzureichend umgesetzt worden (nach *Bachmeier*¹³⁰ steht es den Mitgliedsstaaten überhaupt frei, bei der Umsetzung von Art 23 DS-RL zwischen einer Gefährdungs- und Verschuldenshaftung zu wählen).

Ein anderer Standpunkt¹³¹ widerlegt diese Ansicht: Zunächst wird davon ausgegangen, dass die DS-RL eine verschuldensabhängige Verpflichtung zum

¹²⁸ EuGH 14.7.1994, Rs C-91/92, Faccini Dori, Slg 1994, I-3325; EuGH 7.3.1996, Rs C-192/94, El Corte Ingles, Slg 1996, I-1281.

¹²⁹ *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art 23 Rz 6; *Lackner*, Die Entwicklung des wirtschaftsrechtlichen Datenschutzes in Österreich unter besonderer Berücksichtigung des Datenschutzgesetzes 2000 (2001) 77; *Moser*, Datenschutzgesetz 2000 und Implementierung bei der Versicherungsanstalt des österreichischen Bergbaues (2001) 42.

¹³⁰ *Bachmeier*, EG-Datenschutzrichtlinie – Rechtliche Konsequenzen für die Datenschutzpraxis, RDV 1995, 49 (51).

¹³¹ *Ehmann/Helfrich*, EG Datenschutzrichtlinie (1999) Art 23 Rz 11ff; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz § 33 Pkt 3; *Kopp*, Der EG-Richtlinienvorschlag zum Datenschutz in Europa, DuD 1993,

Schadenersatz offen lässt. Aus der Formulierung des Abs 1 könne man in der Tat leicht eine Gefährdungshaftung unabhängig vom Verschulden des für die Verarbeitung Verantwortlichen vermuten. Um zum korrekten Ergebnis zu kommen dürfe man jedoch Abs 1 nicht isoliert, sondern im Zusammenspiel mit Abs 2 betrachten, der für den für die Verarbeitung Verantwortlichen eine Haftungsbefreiung vorsieht, wenn diesem der Nachweis gelingt, dass ihm der den Schaden verursachende Umstand nicht zur Last gelegt werden kann - es kommt somit zu einer Umkehr der Beweislast (die im übrigen in § 33 Abs 3 DSG 2000 normiert ist). Hätte der Richtliniengeber tatsächlich statt einer Verschuldenshaftung eine Gefährdungshaftung im Sinn gehabt, so würde die Regelung des Art 23 Abs 2 der DS-RL keinen Sinn ergeben, weil diese ja gerade auf das Verschulden des für die Verarbeitung Verantwortlichen abstellt.

Unter Berücksichtigung von Abs 2 empfiehlt es sich richtigerweise also, Art 23 Abs 1 der DS-RL dahingehend auszulegen, dass es nach dem Willen des Richtliniengebers sehr wohl zu einer verschuldensabhängigen Haftung kommen soll; dieser Ansicht ist im übrigen der österreichische Gesetzgeber gefolgt, der ja in § 33 Abs 1 DSG 2000 ausdrücklich von einer „schuldhaften“ Verletzung des DSG 2000 spricht. Somit scheint Art 23 DS-RL durchaus richtlinienkonform umgesetzt worden zu sein.

5.2 Immaterielle Schäden

Auch hinsichtlich der Ersatzpflicht für immaterielle Schäden ist zu hinterfragen, ob die DS-RL korrekt ins nationale Recht transformiert worden ist. Eine in der Lehre vertretene Ansicht (vertreten ua von *Dammann/Simitis*¹³²) geht davon aus, dass aufgrund der Tatsache, dass die DS-RL in Art 23 keine näheren Konkretisierungen macht, sowohl materielle als auch immaterielle Schäden zu einer generellen Ersatzpflicht führen würden. Demzufolge wäre die Vorschrift des § 33 Abs 1 zweiter Satz DSG 2000 gemeinschaftsrechtswidrig, weil sie eine generelle Ersatzpflicht immaterieller Schäden ausschließt und nur für jene Fälle vorsieht, in

11 (14); *Schneider*, Die EG-Richtlinie zum Datenschutz, CR 1993, 35 (39); *Souhrada-Kirchmayer*, Der Vorschlag einer allgemeinen EG-Datenschutzrichtlinie und seine Auswirkungen auf das österreichische DSG, JBI 1995, 147 (155); *Weiss*, Datenschutzrecht in der EU, FJ 1998, 7 (9); *Duschanek*, ZfV 2000, 536.

¹³² *Dammann/Simitis*, EG-Datenschutzrichtlinie Art 23 Rz 5; *Brühmann/Zerdick*, Umsetzung der EG-Datenschutzrichtlinie, CR 1996, 429 (435); *Kopp*, Das EG-Richtlinienvorhaben zum Datenschutz, RDV 1993, 1 (8).

denen die öffentlich zugängliche Verwendung der in § 18 Abs 2 Z 1 bis 3 genannten Datenarten zu einer Verletzung schutzwürdiger Geheimhaltungsinteressen führt, die einer Bloßstellung iSd § 7 MedG gleichkommt.

*Ehmann/Helfrich*¹³³ sehen die Lage differenzierter: Zunächst sei davon auszugehen, dass ein Schaden zu ersetzen sei, wobei offen bleibt, ob immaterielle Schäden miteingeschlossen sind. Die Formulierung der DS-RL müsse sowohl nach dem Wortlaut als auch vor dem Hintergrund nationaler Schadenersatzregelungen interpretiert werden. In Anbetracht der Tatsache, dass Art 23 Abs 1 der DS-RL keine ausdrückliche Regelung bezüglich des Ersatzes von immateriellen Schäden enthält, sei den Mitgliedsstaaten ein Umsetzungsspielraum überlassen worden, der es dem nationalen Gesetzgeber freistellt, ob dieser den Ersatz immaterieller Schäden zwingend vorsieht. Im österreichischen Rechtssystem stellt der Ersatz von immateriellen Schäden jedenfalls bloß die Ausnahme von der Regel dar (eine Ersatzpflicht besteht nur dort, wo diese ausdrücklich vorgesehen ist) und ist grundsätzlich nicht vorgesehen. Ehmann/Helfrich gehen davon aus, dass die DS-RL keinen ausdrücklichen Ersatz von immateriellen Schäden vorsieht. Dennoch werde „der nationale Gesetzgeber – nicht zuletzt auch aus Gründen der innereuropäischen Gleichbehandlung datenschutzrechtlicher Haftungsrisiken – im Rahmen der Umsetzung die Gelegenheit ergreifen müssen, zur Frage der Ersatzfähigkeit immaterieller Schäden gesetzgeberisch Stellung zu beziehen“. Zudem böte erst eine realistische durchsetzbare zivilrechtliche Sanktion in Gestalt von immateriellem Schadenersatz in pauschalierter Form einen hinreichenden Anreiz, der Wahrung des Datenschutzes hinreichende Aufmerksamkeit zu schenken.

Der Ersatz von immateriellen Schäden ist also durch die DS-RL nicht ausdrücklich vorgesehen, der österreichische Gesetzgeber hat jedoch von seinem Umsetzungsspielraum Gebrauch gemacht und (zusätzlich zu der Ersatzpflicht von materiellen Schäden) auch eine Ersatzpflicht von immateriellen Schäden in der Gestalt des § 33 Abs 1 S 2 DSG 2000 vorgesehen, bei der die öffentlich zugängliche Verwendung bestimmter Kategorien personenbezogener Daten einer

Bloßstellung nach § 7 MedG gleichkommt. Insofern erscheint auch im Hinblick darauf, dass nicht generell jede Art von immateriellen Schäden zu einer Haftung führt, Art 23 DS-RL richtlinienkonform umgesetzt worden zu sein.

5.3 Legitimation zur Geltendmachung

Ein weiterer Aspekt einer möglichen Gemeinschaftsrechtswidrigkeit von § 33 ist die Frage, welche Personen zur Geltendmachung eines durch die Verwendung personenbezogener Daten erlittenen Schadens legitimiert sind. *Ghali*¹³⁴ legt Art 23 DS-RL dahingehend aus, dass nicht nur die betroffenen Personen selbst, sondern auch jene Personen, die einen Schaden aufgrund der Verarbeitung personenbezogener Daten Dritter erleiden, zur Geltendmachung von Schadenersatzansprüchen aufgrund der DS-RL berechtigt sind. Nach dieser Ansicht wäre § 33 DSG 2000 gemeinschaftsrechtswidrig, da in dessen Abs 1 ausdrücklich nur der Betroffene (das ist gem § 4 Z 3 DSG 2000 jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden, siehe dazu näher Kapitel 3.1.2) zur Geltendmachung von Schadenersatzansprüchen legitimiert wird. Zwar verweist § 33 Abs 1 auf die allgemeinen Schadenersatzregelungen des ABGB, auf die ein Außenstehender, dem durch die Verarbeitung von personenbezogenen Daten dritter Personen ein Schaden entstanden ist, ebenfalls seine Ansprüche stützen könnte – jedoch käme der Außenstehende in diesem Fall nicht in den Genuss der in Art 23 Abs 2 DS-RL normierten und in § 33 Abs 3 DSG 2000 in österreichisches Recht umgesetzten Beweislastumkehr zugunsten des Betroffenen. Nutznießer dieser Umkehr der Beweislast ist nämlich ausschließlich eine Person, deren personenbezogene Daten verwendet worden sind (somit der Betroffene iSd § 4 Z 3) und eben nicht eine Person, der bloß durch die Verwendung von personenbezogener Daten Dritter ein Schaden entstanden ist. Auf die restlichen Vorteile einer Betroffeneneneigenschaft iSd DSG 2000 im Hinblick auf Schadenersatzforderungen (Möglichkeit der Geltendmachung von immateriellen Schäden nach § 33 Abs 1 S 2 DSG 2000 sowie die analoge Anwendung der Gehilfenhaftung nach § 1313a ABGB auch ohne vertragliche Beziehung zwischen Auftraggeber und Betroffenen nach Abs 2) braucht in diesem

¹³³ Ehmman/Helfrich, Datenschutzrichtlinie Art 23 Rz 20ff; in die gleiche Richtung gehend *Schneider*, CR 1993, 35, *Souhrada-Kirchmayer*, JBl 1995, 155.

¹³⁴ *Ghali*, Datenschutz 279.

Zusammenhang nicht näher eingegangen zu werden, da diese nicht durch Art 23 DS-RL gewährt werden, sondern im Ermessen des nationalen Gesetzgebers (Umsetzungsspielraum) stehen.

Es stellt sich demnach die Frage, ob nicht nur der Betroffene selbst, sondern auch ein Dritter zur Geltendmachung von Schadenersatzansprüchen aufgrund der DS-RL berechtigt ist. Gegen die von *Ghali* vertretene Ansicht spricht zum einen Erwägungsgrund 55 der DS-RL: „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“ Eine „betroffene Person“ ist nach Art 2 lit a DS-RL eine bestimmte oder bestimmbare natürliche Person und somit jemand, dessen personenbezogene Daten verwendet werden. Erwägungsgrund 55 zielt also nur auf die Berechtigung zur Geltendmachung von Schadenersatzansprüchen von Betroffenen ab; zudem spricht Erwägungsgrund 26 davon, dass die Schutzprinzipien für alle Informationen über eine bestimmte oder bestimmbare Person gelten und hat ebenfalls nicht den Schutz Dritter zum Inhalt. Demnach ist Art 23 DS-RL keinesfalls dahingehend auszulegen, dass auch Außenstehenden – trotz der Verwendung personenbezogener Daten Dritter – der Vorteil der Beweislastumkehr des Abs 2 gewährt werden soll.

Zum anderen ist auch Bedacht darauf zu nehmen, wer überhaupt Schutzobjekt datenschutzrechtlicher Vorschriften wie der DS-RL oder des DSG 2000 sein soll: Gem Art 1 DS-RL gewährleisten die Mitgliedsstaaten den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Geschützt werden sollen also die datenschutzrechtlich Betroffenen. Auch Erwägungsgrund 10 stellt klar, dass der Schutzgegenstand der nationalen Datenschutzvorschriften die Gewährleistung der Achtung der Grundrechte und –freiheiten, insbesondere auch das in Art 8 MRK sowie in den allgemeinen Grundsätzen des

Gemeinschaftsrechts anerkannte Recht auf die Privatsphäre ist. Schutzobjekte der DS-RL sind demnach also die betroffenen Personen, deren personenbezogenen Daten verarbeitet werden.

Es ist folglich nicht einzusehen, dass auch Außenstehende, die durch die Verwendung personenbezogener Daten Dritter einen Schaden erlitten haben, in den Genuss der Beweislastumkehr des Art 23 Abs 2 DS-RL kommen sollen, da diese vom Schutzzweck der DS-RL nicht umfasst sind und zudem etwaige Ansprüche auch nach den allgemeinen nationalen Schadenersatzregeln geltend machen können (in Österreich wäre ein auf diese Art Geschädigter auf die allgemeinen Regelungen des ABGB in Gestalt der §§ 1293ff zu verweisen; die Beweislastumkehr des § 1298 käme nur in Fällen einer vertraglichen Beziehung zwischen geschädigtem Dritten und dem Auftraggeber in Betracht). Somit erscheint § 33 Abs 1 DSG 2000 auch hinsichtlich der Legitimation von Schadenersatzansprüchen durchaus im Einklang mit dem Gemeinschaftsrecht zu stehen.

5.4 Wortlaut des § 33 DSG 2000

Kritik scheint am Wortlaut des § 33 angebracht zu sein: Nach dessen Formulierung in Abs 1 ist eine „schuldhaft“ Verletzung Anspruchsvoraussetzung für den Ersatz von Schäden, gleichzeitig wird auf die allgemeinen Regelungen des ABGB verwiesen. Die §§ 1293ff fordern aber ohnehin das Vorliegen eines Verschuldens, womit die neuerliche Normierung desselben in § 33 Abs 1 DSG 2000 nicht nochmals nötig gewesen wäre. Auch ist die Umkehr der Beweislast zugunsten des Betroffenen in Abs 3 umständlich formuliert worden („*Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm ... nicht zur Last gelegt werden kann*“) und hätte klarer und verständlicher umschrieben werden können (etwa durch „Die Beweislast des rechtmäßigen Verhaltens obliegt dem Auftraggeber“). Des Weiteren erscheint der Ausdruck „Leute des Auftraggebers“ zunächst klärungsbedürftig und hätte wohl in Bezugnahme auf § 1313a ABGB treffender umschrieben werden können.

Die Anspruchsvoraussetzung der „Schuldhaftigkeit“ erscheint jedoch auch aus einer anderen Perspektive zweifelhaft: *Koziol*¹³⁵ weist darauf hin, dass die Möglichkeit des Nachweises nach Abs 3 (nämlich dass sich der Auftraggeber bzw Dienstleister von seiner Haftung befreien kann, falls der zum Schaden führende Umstand weder ihm, noch seinen Leuten zur Last gelegt werden kann) ins Leere führt, würde man das Verschulden nach Abs 1 tatsächlich als Anspruchsvoraussetzung sehen; denn kann der schädigende Umstand dem Auftraggeber (Dienstleister) tatsächlich nicht zur Last gelegt werden, so hat er ohnehin nicht schuldhaft gehandelt, womit die grundsätzliche Anspruchsvoraussetzung nach Abs 1 von vornhinein nicht gegeben wäre und die Möglichkeit des Nachweises nach Abs 3 ad absurdum geführt würde. Es erscheint somit sinnvoll, Abs 1 so zu interpretieren, dass die „Schuldhaftigkeit“ der Verletzung nicht als Anspruchsvoraussetzung zu verstehen ist, sondern etwa als Klarstellung des Gesetzgebers, dass es zu keiner Gefährdungs-, sondern zu einer Verschuldenshaftung kommen soll.

5.5 Kritische Gesamtbetrachtung des § 33 DSGVO 2000

Zusammenfassend ist zu sagen, dass Art 23 der DS-RL in Gestalt des § 33 DSGVO 2000 trotz teilweise gegenteiliger Auslegung in der Lehre richtlinienkonform umgesetzt und ins nationale Recht transformiert worden ist. Das Hereinnehmen einer „schuldhaften“, dem DSGVO 2000 widrigen Verwendung von personenbezogenen Daten als Anspruchsvoraussetzung für den Ersatz des Schadens erscheint jedoch im Zusammenhang mit Abs 3 zumindest unglücklich formuliert zu sein und auch andere Ausdrücke hätten wohl (ohne größeren Aufwand) eindeutiger gewählt werden können um Unklarheiten bei der Auslegung einzelner Begriffe beseitigen zu können. Es wäre wünschenswert, wenn der Gesetzgeber einzelne Passagen des § 33 neu formulieren und für mehr Klarheit für den Rechtsanwender sorgen würde.

¹³⁵ *Koziol*, Ein europäisches Schadenersatzrecht – Wirklichkeit und Traum, JBl 2001, 29 (31).

6. Schadenersatz für den Bruch des Datengeheimnisses im öffentlichen Bereich

Wie eingangs erwähnt kommt eine Geltendmachung von Schadenersatzansprüchen nach § 33 DSG 2000 nur dann in Frage, wenn der Auftraggeber dem privaten Bereich zuzurechnen ist oder es sich um einen Bereich der Privatwirtschaftsverwaltung handelt; stammt der Auftraggeber der Datenanwendung aus dem öffentlichen Bereich (Gerichtsbarkeit oder Hoheitsverwaltung), so ist § 33 nicht anzuwenden, sondern es greifen die allgemeinen Regelungen der Amts- und Organhaftung ein.

Die grundsätzliche Regelung für die Haftung der Träger der hoheitlichen Verwaltung enthält Art 23 B-VG, zur näheren Ausführung wurden das AHG und das OrgHG erlassen. Gem § 1 Abs 1 AHG haften die Rechtsträger (Bund, Länder, Bezirke, Gemeinden, sonstige Körperschaften öffentlichen Rechts, Träger der Sozialversicherung) nach den Bestimmungen des bürgerlichen Rechts für Schäden an der Person oder am Vermögen, die ihre Organe in Vollziehung der Gesetze durch ein rechtswidriges Verhalten schuldhaft zugefügt haben. Dabei kommt es zu keiner grundsätzlichen Naturalrestitution nach § 1323 ABGB, sondern zu einem Ersatz in Geld. Es handelt sich um einen funktionellen Organbegriff.¹³⁶ „Organ“ ist demnach unabhängig ua von der Dauer der Ernennung oder ihrer Stellung zum Rechtsträger jede Person, die in Vollziehung der Gesetze handelt. Absolut ausgeschlossen sind nach § 2 Abs 3 AHG aus einem Erkenntnis des VfGH, des VwGH oder des OGH abgeleitete Schadenersatzansprüche sowie Fälle, in denen der Geschädigte den Eintritt des Schadens durch ein Rechtsmittel oder durch Beschwerde an den VwGH abwenden hätte können. Zudem verjähren etwaige Ansprüche gem § 6 Abs 1 binnen drei Jahren ab Kenntnis des Schadens beim Geschädigten (unbeachtet der Kenntnis des Schädigers) bzw nach zehn Jahren. Die Geltendmachung des Anspruchs erfolgt mittels Klage gegen den Rechtsträger beim Landesgericht, in dessen Sprengel die Rechtsverletzung begangen worden ist (§ 9 Abs 1).

¹³⁶ *Walter/Mayer*, Grundriß⁹ Rz 1285.

Die Gesetzesmaterialien liefern keine Klarheit darüber, ob hinsichtlich der Amtshaftung im öffentlichen Bereich neben den allgemeinen Bestimmungen des bürgerlichen Rechts auch die Regelung bezüglich des Ersatzes von immateriellen Schäden nach § 33 Abs 1 zweiter Satz DSG 2000 sowie die Beweislastumkehr des Abs 3 zur Anwendung kommen sollen, was im AHG nicht ausdrücklich vorgesehen ist, da es im Anwendungsbereich des AHG grundsätzlich zu einer Haftung nach den §§ 1293ff ABGB kommen soll. *Schrage*¹³⁷ meint, dass das Gesetz den Umfang der Haftung im privaten und öffentlichen Bereich nicht unterschiedlich gestalten wollte; vielmehr dürfte eine unbeabsichtigte Gesetzeslücke vorliegen. Diese sei so zu schließen, dass bei Datenschutzverletzungen im hoheitlichen Bereich die gleiche Haftung wie nach § 33 DSG 2000 einzutreten habe und insoweit der Amtshaftungsanspruch als erweitert anzusehen sei (in die gleiche Richtung geht *Duschanek*¹³⁸). Somit hat der Betroffene auch gegen einen Auftraggeber des öffentlichen Bereichs analog zu § 33 DSG 2000 eine Möglichkeit zur Geltendmachung von immateriellen Schäden und kommt in den Genuss der Beweislastumkehr zu seinen Gunsten.

Organe des Bundes, eines Landes, eines Bezirks, eines Gemeindeverbandes, einer Gemeinde, eines Trägers der Sozialversicherung oder einer sonstigen Körperschaft oder Anstalt öffentlichen Rechts haften (analog zur Amtshaftung) gem § 1 Abs 1 OrgHG nach den Bestimmungen des bürgerlichen Rechts für Schäden am Vermögen, die sie dem Rechtsträger, als dessen Organ sie gehandelt haben, in Vollziehung der Gesetze unmittelbar durch ein schuldhaftes und rechtswidriges Verhalten zugefügt haben. Es gelten die gleichen Ausschließungsgründe wie nach dem AHG (Erkenntnis des VfGH, des VwGH oder des OGH bzw Möglichkeit eines Rechtsmittels oder Beschwerde an den VfGH/VwGH) und auch hinsichtlich der Verjährung sieht § 5 OrgHG die gleichen Bestimmungen wie § 6 Abs 1 AHG vor.

¹³⁷ *Schrage*, Kommentar³ Rz 13.

¹³⁸ *Duschanek*, ZfV 2000, 536.

7. Schlussfolgerungen

Der Handlungsbedarf des Gesetzgebers, der durch die DS-RL gegeben war, hat zwar Grundzüge des österreichischen Datenschutzrechts (wie etwa die Konzeption der Normierung eines Grundrechts auf Datenschutz mit einfachgesetzlicher näherer Ausgestaltung) beibehalten, jedoch wurde das DSG 1978 vom DSG 2000 abgelöst und damit wurden die gesetzlichen Rahmenbedingungen für die Verarbeitung personenbezogener Daten zum Teil erheblich geändert. So wurde die bisherige Zweiteilung in einen öffentlichen und in einen privaten Bereich aufgegeben, die Registrierungsspflichten beim DVR wurden wesentlich reduziert und auch im Bereich des Rechtsschutzes ist es zu Erleichterungen für den Betroffenen gekommen. So hat die DSK nunmehr auch im privaten Bereich eine erweiterte Zuständigkeit bei Verletzungen des Rechts auf Auskunft, und auch hinsichtlich der Geltendmachung etwaiger Schadenersatzansprüche genießt der Betroffene mehrere Vorteile abweichend von den allgemeinen Haftungsregeln des ABGB: Nicht dem Geschädigten, sondern dem Auftraggeber einer Datenanwendung obliegt die Beweislast; weiters kommt es zu einer Ausdehnung der Haftung des Auftraggebers auf seinen Dienstleister und dessen Leute analog zur Erfüllungsgehilfenhaftung nach § 1313a ABGB auch in jenen Fällen, in denen der Auftraggeber sonst nur nach der Besorgungsgehilfenhaftung nach § 1315 zur Verantwortung gezogen werden könnte. Erfreulicherweise werden unter bestimmten Voraussetzungen auch immaterielle Schäden pauschal ersetzt und so ist eine Verletzung des Datengeheimnisses auch wirkungsvoll sanktioniert, was im Hinblick auf die immer weiter fortschreitende weltweite Vernetzung äußerst wichtig erscheint; auch (und gerade) im Computerzeitalter hat der einzelne Mensch ein Recht auf Privatsphäre.

Trotz teilweise abweichender Meinungen in der Literatur ist die DS-RL bezüglich der Schadenersatzregelung des § 33 DSG 2000 korrekt umgesetzt worden; eine verschuldensabhängige Haftung und eine auf Fälle einer Bloßstellung nach § 7 MedG eingeschränkte Ersatzpflicht für immaterielle Schäden steht durchaus im Einklang mit Art 23 DS-RL.

Hinsichtlich des Wortlautes des § 33 hätte der Gesetzgeber jedoch eindeutiger Formulierungen verwenden können. Ausdrücke wie „Leute des Auftraggebers“ oder die Formulierung der Beweislastumkehr des Abs 3 bedürfen nämlich zunächst einer näheren Klärung und sind vor allem für Laien nur schwer verständlich. Es ist zu hoffen, dass der Gesetzgeber im Zuge einer Novelle für mehr Klarheit und Rechtssicherheit sorgt.

Insgesamt ist es zu begrüßen, dass sich der (europäische) Gesetzgeber dazu entschlossen hat der schon seit Erlassung des DSG 1978 bestehenden Forderung nach einer Normierung von bereichsspezifischen Schadenersatzregelungen im Datenschutzrecht nachzukommen. Verschiedenste Stellen sammeln mehr und mehr Daten über den einzelnen Bürger und vielfach wird dieser wohl mangels Kenntnis gar nicht merken, dass seine personenbezogenen Daten ohne seine Zustimmung und entgegen den gesetzlichen Regeln verwendet worden sind. Deswegen scheint es nur billig, dem Betroffenen gewissermaßen als Ausgleich die Geltendmachung von Schadenersatzansprüchen zu erleichtern. Auch kann § 33 als Präventions-Norm gesehen werden: Auftraggeber sollen sich der Tatsache bewusst werden, dass eine datenschutzrechtswidrige Verarbeitung von personenbezogenen Daten durchaus zu einer Haftung des Auftraggebers führen kann und so überlegt man es sich eventuell zweimal, bevor man vorsätzlich oder aber nur fahrlässig das Datengeheimnis verletzt. Gerade durch die Möglichkeit des Ersatzes von immateriellen Schäden ist zu hoffen, dass Auftraggeber sozusagen zur Befolgung des Datenschutzes „erzogen“ werden und ein Prozessrisiko nicht so einfach in Kauf nehmen.

Es ist zu hoffen, dass die Schadenersatzregelung des § 33 in der Praxis nicht totes Recht bleibt, sondern dass in Zukunft Betroffene öfter von ihrem Recht Gebrauch machen. Die bisher so gut wie nicht vorhandene Rechtsprechung zu dieser Norm lässt jedenfalls befürchten, dass die Erhebung einer Schadenersatzklage (noch dazu vor dem LG) eine nicht unbeträchtliche Hürde für den einzelnen Betroffenen darstellt, die ihn von der Geltendmachung seiner Rechte abhält.

Mit dem DSG 2000 hat der Datenschutz in Österreich jedenfalls eine ausreichende gesetzliche Absicherung erfahren. Jedoch ist gerade in Zeiten einer sich schnell weiterentwickelnden Computer- und High Tech-Industrie darauf zu achten, dass die gesetzgeberische mit der technischen Entwicklung standhält, um den Betroffenen auch weiterhin ein ausreichendes Niveau an Datenschutz zu gewährleisten. Neue Technologien werden ständig entwickelt und Gleiches sollte auch für den Datenschutz gelten, damit die Schreckensvision des „gläsernen Menschen“ nicht eines Tages Realität wird.

Literaturverzeichnis

- Adamovich Ludwig K./Funk Bernd-Christian*, Allgemeines Verwaltungsrecht³
(Wien – New York 1987)
- Bachmeier Roland*, EG-Datenschutzrichtlinie – Rechtliche Konsequenzen für die
Datenschutzpraxis, RDV 1995, 49
- Berka Walter/Höhne Thomas/Noll Alfred J./Polley Ulrich*, Mediengesetz
Praxiskommentar (Wien 2002)
- Brandstetter Ulrich/Schmid Helmut*, Kommentar zum Mediengesetz² (Wien 1999)
- Brühmann Ulf/Zerdick Thomas*, Umsetzung der EG-Datenschutzrichtlinie,
CR 1996, 429
- Dammann Ulrich/Simitis Spiros*, EG-Datenschutzrichtlinie (Baden-Baden 1997)
- Dohr Walter/Pollirer Hans-Jürgen/Weiss Ernst M.*, Datenschutzrecht² (Wien 2002)
- Drobesch Heinz/Grosinger Walter*, Das neue österreichische Datenschutzgesetz
(Wien 2000)
- Duschanek Alfred*, Neuerungen und offene Fragen im Datenschutzgesetz 2000,
ZfV 2000, 526
- Duschanek Alfred/Rosenmayr-Klemenz Claudia*, Datenschutzgesetz-
Regierungsvorlage, ecolex 1999, 361
- Duschanek Alfred/Rosenmayr-Klemenz Claudia*, Datenschutzgesetz 2000 (Wien
2000)
- Ehmann Eugen/Helfrich Marcus*, EG Datenschutzrichtlinie (Köln 1999)
- Ermacora Felix*, Grundriß der Menschenrechte in Österreich (Wien 1988)
- Foregger Egmont/Litzka Gerhard*, Mediengesetz⁴ (Wien 2000)
- Ghali Yvonne*, Datenschutz Rechtsgrundlagen (Wien 1999)
- Jahnel Dietmar*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49
- Jahnel Dietmar/Schramm Alfred/Staudegger Elisabeth* (Hrsg), Informatikrecht²
(Wien – New York 2003)
- Kilches Ralph*, Datenschutzgesetz 2000 – Selbstbestimmter Datenschutz,
MR 1999, 261
- Koitz Rainer*, Informatikrecht schnell erfasst (Berlin 2002)
- Kopp Ferdinand*, Das EG-Richtlinienvorhaben zum Datenschutz, RDV 1993, 1

Kopp Ferdinand, Der EG-Richtlinienvorschlag zum Datenschutz in Europa, DuD 1993, 11

Koziol Helmut, Österreichisches Haftpflichtrecht I³ (Wien 1997)

Koziol Helmut, Ein europäisches Schadenersatzrecht – Wirklichkeit und Traum, JBI 2001, 29

Koziol Helmut/Welser Rudolf, Grundriss des bürgerlichen Rechts II¹² (Wien 2001)

Lackner Erich, Die Entwicklung des wirtschaftsrechtlichen Datenschutzes in Österreich unter besonderer Berücksichtigung des Datenschutzgesetzes 2000 (Innsbruck 2001)

Mayer-Schönberger Viktor/Brandl Ernst O., Datenschutzgesetz 2000 (Wien 1999)

Moser Kathrin, Datenschutzgesetz 2000 und Implementierung bei der Versicherungsanstalt des österreichischen Bergbaues (Graz 2001)

Öhlinger Theo, Verfassungsrecht⁵ (Wien 2003)

Reimann Karin, Der Datenschutz in Österreich – vom Datenschutzgesetz 1978 bis zum Datenschutzgesetz 2000 (Graz 2001)

Schneider Jochen, Die EG-Richtlinie zum Datenschutz, CR 1993, 35

Schrager Walter, Kommentar zum Amtshaftungsgesetz³ (Wien 2003)

Schwimann Michael (Hrsg), Praxiskommentar zum ABGB VII² (Wien 1997)

Souhrada-Kirchmayer Eva, Der Vorschlag einer allgemeinen EG-Datenschutzrichtlinie und seine Auswirkungen auf das österreichische DSG, JBI 1995, 147

Souhrada-Kirchmayr Eva, Das Datenschutzgesetz 2000, SozSi 2000, 938

Tinnefeld Marie-Theres/Tubies Helga, Datenschutzrecht² (München – Wien 1989)

Walter Robert/Mayer Heinz, Grundriß des österreichischen Bundesverfassungsrechts⁹ (Wien 2000)

Weiss Ernst, Datenschutzrecht in der EU, FJ 1998, 7

Anhang

§ 33 DSG 2000

§ 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.

Artikel 23 DS-RL

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.