universität wien

DISSERTATION

Titel der Dissertation

Das Grundrecht auf Datenschutz im Unternehmen unter besonderer Berücksichtigung gesellschaftsrechtlicher Umstrukturierungen

Verfasser

Mag. iur. Maximilian Auer

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr. iur.)

Wien, 2009

Studienkennzahl lt. Studienblatt:	A 083 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuerin / Betreuer:	Ao. Univ.-Prof. Dr. Gerhard Strejcek

Vorwort

Gegenstand dieser Arbeit ist das Grundrecht auf Datenschutz im Unternehmen unter besonderer Berücksichtigung gesellschaftsrechtlicher Umstrukturierungen. Es erscheint dem Autor angebracht die Gründe und Überlegungen, die zu dieser Themenwahl geführt haben zu Beginn kurz darzulegen.

Das Thema Datenschutz gewinnt in der Fachliteratur zunehmend an Raum und hat sich mittlerweile unter den verschiedensten Fragestellungen von einem Randgebiet in das Zentrum juristischer Kontroverse bewegt. Lange Zeit wurde dem Datenschutzrecht, sowohl im Schrifttum als auch in der Praxis, eine eher untergeordnete Bedeutung zugemessen. Dieser Umstand lässt sich auf mehrere Ursachen zurückführen: Zum einen muss bemerkt werden, dass sich die Bestimmungen des DSG für damit in der Praxis konfrontierte Nichtjuristen großteils abstrakt und kompliziert darstellen.

Damit macht sich bedauerlicherweise gerade bei solchen Unternehmen, für die die Datenverarbeitung einen wesentlichen Teil ihres Geschäftsfeldes ausmacht, eine gewisse Aversion gegen den Datenschutz bemerkbar. Zum anderen muss bei den von Datenverarbeitungen Betroffenen nach wie vor ein generell fehlendes Bewusstsein, was die Problematik einer oftmals allzu bereitwilligen Zurverfügungstellung personenbezogener Daten betrifft, konstatiert werden.

Es ist mittlerweile zur Tatsache geworden, dass die moderne Informations- und Kommunikationstechnologie in beinah alle Bereiche des menschlichen Alltagslebens Einzug gehalten hat. Es werden in fast allen Lebenssituationen des Menschen Computer zur Bewältigung derselben eingesetzt.

Mit den unbestrittenen zahlreichen Vereinfachungen und positiven Effekten, die diese Entwicklung mit sich gebracht hat, gehen jedoch auch Gefahren einher, die sich durch die automatische Verarbeitung großer Mengen personenbezogener Daten ergeben können. Insb die massenhafte Verwertung dieser Daten durch Unternehmen der Privatwirtschaft als Gut in einer globalisierten Wirtschaft stellt den Gesetzgeber vor die Aufgabe flankierend entsprechende gesetzliche Schutzmaßnahmen zu schaffen.

Dabei ist einerseits das Erfordernis zu beachten die Regelungen so zu gestalten, dass ein vernünftiger Ausgleich zwischen den schutzwürdigen Interessen des Einzelnen, von der Datenverarbeitung Betroffenen, und allgemeinen Interessen an einer Modernisierung und Vereinfachung der verschiedenen Lebensbereiche geschaffen wird.

Andererseits müssen die entsprechenden Regelungen den Anforderungen einer sich stetig entwickelnden und verändernden Materie Rechnung tragen. Die solcherart notwendige Flexibilität der gesetzlichen Vorschriften stellt nicht selten eine legistische Schwierigkeit dar und erklärt auch die mitunter als nicht ganz eindeutig empfundenen Formulierungen der Vorschriften zum Datenschutzrecht.

Nichtsdestotrotz ist der Datenschutz besonders im wirtschaftlichen Rechtsalltag längst zu einem nicht mehr wegzudenkenden Faktor geworden. Beinah jede unternehmerische Tätigkeit weist Berührungspunkte zu diesem Regelungsgegenstand auf. Die Privatsphäre und Persönlichkeit des einzelnen Menschen im Rahmen wirtschaftlicher Betätigungen, der elektronische Geschäftsverkehr sowie zahlreiche vertragliche Gestaltungserfordernisse lassen dem Schutz personenbezogener Daten eine immer größer werdende Bedeutung zukommen.

Es sind va das Spannungsfeld von Transparenz und Schutz der Vertraulichkeit sowie die vielfältigen Beziehungen, die sich in diesem Zusammenhang zu den einzelnen Gruppen von Betroffenen ergeben, die eine Behandlung des Themas Datenschutz im Unternehmen lohnend machen.

Ein Schwerpunkt wird hierbei auf den Vorgang gesellschaftsrechtlicher Umstrukturierungen gelegt. Der Erwerb von Unternehmen, bzw von Anteilen an solchen, gehört in der Wirtschaft mittlerweile zum täglichen Geschäft. Damit gehen zumeist zwangsläufig Veränderungen in den rechtlichen Strukturen der Unternehmen einher (zB im Rahmen von Verschmelzungen), insb werden bei diesen Vorgängen oftmals große Mengen personenbezogener Daten verwendet.

Die für den Kaufinteressenten besonders wichtige Information über die wirtschaftlichen Umstände des entsprechenden Unternehmens erfolgt dabei im Rahmen sog Due Diligence Prüfungen. Im Zuge derer kann gerade die umfassende Zurverfügungstellung

personenbezogener Daten wesentliche Voraussetzung für den Erfolg einer geplanten Akquisition sein. Die Untersuchung des datenschutzrechtlichen Schicksals der dabei verwendeten Informationen ist somit ebenso angezeigt wie sinnvoll.

Weiters werden besondere Fragestellungen im Konzern erörtert sowie ein Überblick über datenschutzrechtlich relevante Sachverhalte in den Bereichen IT-Sicherheit, Arbeitsverhältnis und E-Commerce gegeben. Ein Exkurs widmet sich letztlich dem Datenschutz in der staatlichen Verwaltung im Bezug auf die wirtschaftliche Nutzung der dort verfügbaren Informationen.

Wien, im Oktober 2009 *Maximilian Auer*

Inhaltsverzeichnis

Abkürzungsverzeichnis

§	Paragraph
aA	andere(r) Ansicht
ABGB	Allgemeines bürgerliches Gesetzbuch JGS 946 idF BGBl I 2008/100
Abl	Amtsblatt
abl	ablehnend
Abs	Absatz
AG	Aktiengesellschaft
AktG	Aktiengesetz 1965 BGBl 1965/98 idgF
allg	allgemein
Anm	Anmerkung
AR	Aufsichtsrat
ArbVG	Arbeitsverfassungsgesetz
Art	Artikel
BB	(deutsche Zeitschrift) „Der Betriebsberater“
B2B	Business-to-Business
B2C	Business-to-Customer
BDSG	(deutsches) Bundesdatenschutzgesetz BGBl I S. 66 idgF
BGBl	Bundesgesetzblatt
BKA	Bundeskanzleramt
BlgNr	Beilage(n) zu den stenographischen Protokollen des Nationalrats
Bsp	Beispiel
bspw	beispielsweise
BWG	Bankwesengesetz BGBl 1993/532 idgF
bzw	beziehungsweise
ca	cirka (ungefähr)
d	deutsch, -e, -er, -es
dgl	dergleichen
D	Deutschland
ders	derselbe
dh	das heißt
DRdA	(österreichische Zeitschrift) Das Recht der Arbeit
DSG	Datenschutzgesetz 2000 BGBl I 1999/165 idgF
DStR	(deutsche Zeitschrift) deutsches Steuerrecht
DVR	Datenverarbeitungsregister
DVR-Nr	Datenverarbeitungsregister-Nummer
DVRV 2002	Datenverarbeitungsregister-Verordnung 2002 BGBl II 2002/24
E	Entscheidung
ECG	E-Commerce-Gesetz
ecolex	Fachzeitschrift für Wirtschaftsrecht
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EGMR	Europäischer Gerichtshof für Menschenrechte
EK	Europäische Kommission
EMRK	Europäische Menschenrechtskonvention BGBl 1958/210 idgF
ErläutRV	Erläuterungen zur Regierungsvorlage
etc	et cetera
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum

EU	Europäische Union
ff	und der, die folgenden
FN	Fußnote
FS	Festschrift
gem	gemäß
GesBR	Gesellschaft bürgerlichen Rechts
GesRZ	(österreichische Zeitschrift) Der Gesellschafter
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz über Gesellschaften mit beschränkter Haftung RGBl 1906/58 idgF
GP	Gesetzgebungsperiode
grds	grundsätzlich
hA	herrschende Ansicht
hL	herrschende Lehre
hM	herrschende Meinung
Hrsg	Herausgeber
hrsg	herausgegeben
idaF	in der alten Fassung
idF	in der Fassung
idR	in der Regel
idS	in diesem Sinne
idZ	in diesem Zusammenhang
iE	im Ergebnis
ieS	im engeren Sinn
iglS	im gleichen Sinn
insb	insbesondere
iS(d)	im Sinne (dies, -er, -es)
iVm	in Verbindung mit
IWG	Informationsweiterverwendungsgesetz BGBl I 2005/135 idgF
iwS	im weiteren Sinn
iZm	im Zusammenhang mit
iZw	im Zweifel
Jud	Judikatur
Kap	Kapitel
Komm	Kommentar
krit	kritisch
leg cit	legis citatae (der zitierten Vorschrift)
lit	litera (Buchstabe)
Lit	Literatur
maW	mit anderen Worten
M&A	Mergers and Acquisitions (Unternehmenszusammenschlüsse und Unternehmenskäufe)
mE	meines Erachtens
MedienG	Mediengesetz BGBl 1981/314 idgF
MMR	(deutsche Zeitschrift) MultiMedia und Recht
MR	Medien und Recht
mwN	mit weiteren Nachweisen
Nachw	Nachweis
NJW	(deutsche Zeitschrift) Neue Juristische Wochenschrift
Nov	Novelle
Nr	Nummer

NZG	(deutsche Zeitschrift) Neue Zeitung für Gesellschaftsrecht
oa	oben angeführt
OGH	Oberster Gerichtshof
OG	offene Gesellschaft
österr	österreichisch, -e, -er, -es
PSI	Public Sector Information
RDV	(deutsche Zeitschrift) Recht der Datenverarbeitung
RdW	Österreichisches Recht der Wirtschaft
RL	Richtlinie
Rs	Rechtsache
Rsp	Rechtsprechung
Rz	Randzahl
S	Satz
s	siehe
sog	so genannt, -e, -er, -es
SpaltG	Spaltungsgesetz BGBl 1996/304 idgF
StGB	Strafgesetzbuch BGBl 1974/60 idgF
StGG	Staatsgrundgesetz RGBl 1867/142 idgF
StMV	Standard- und Musterverordnung 2004 BGBl II 2004/312 idgF
str	strittig
SWK	Österreichische Steuer- und Wirtschaftskartei
SZ	„Entscheidungen des österreichischen Obersten Gerichtshofes in Zivil- (und Justizverwaltungs-) sachen“, veröffentlicht von seinen Mitgliedern
TKG	Telekommunikationsgesetz 2003 BGBl I 2003/70 idgF
u	und
ua	a) und andere, -s b) unter anderem
UGB	Unternehmensgesetzbuch dRGBl 1897/219 idgF
UmwG	Umwandlungsgesetz BGBl 1996/304 idgF
uU	unter Umständen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb 1984 BGBl 1984/448 idgF
uzw	und zwar
V	Verordnung
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofs
vgl	vergleiche
VO	Verordnung
wbl	„wirtschaftsrechtliche blätter“, Zeitschrift für österreichisches und europäisches Wirtschaftsrecht
zB	zum Beispiel
Z	Ziffer
ZAS	Zeitschrift für Arbeitsrecht und Sozialrecht
ZHR	(deutsche) „Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
zT	zum Teil
zutr	zutreffend

I. Einleitung

Die Datenschutzrechtlichen Implikationen, die iZm unternehmerischer Tätigkeit auftreten können, sind notwendigerweise stets im Kontext der historischer Entwicklung dieser Regelungsmaterie zu betrachten. Zum besseren Verständnis wird daher in Folge ein kurzer Überblick über die Entwicklung dieses Rechtsgebietes in Österreich gegeben.

A. Die Entwicklung des Datenschutzrechtes in Österreich

1. Datenschutzrecht in Österreich

Seit nunmehr knapp drei Jahrzehnten besteht in Österreich ein gesetzlich verankerter Datenschutz. Mit Inkrafttreten des ersten österreichischen Datenschutzgesetzes, dem Datenschutzgesetz vom 18. Oktober 1978 (DSG 1978), am 01.01.1980 wurde ein verfassungsgesetzlich gewährleistetes Recht auf Datenschutz implementiert.[1] Mit diesem Gesetz wurde in Österreich erstmals eine umfassende gesetzliche Regelung über die Behandlung personenbezogener Daten geschaffen.[2] Bis zu diesem Zeitpunkt war die Verarbeitung von Informationen beinahe keinen gesetzlichen Beschränkungen unterworfen. Der österreichische Gesetzgeber folgte damit einem gesamteuropäischen Trend zur Implementierung eines Schutzes personenbezogener Daten.

Mit *Mayer-Schönberger/Brandl*[3] lassen sich in diesem Stadium der Rechtsentwicklung die grds Erfordernisse des gesetzlichen Datenschutzes in den späten 1970er Jahren des vergangenen Jahrhunderts wie folgt erkennen: Als Reaktion auf die Bestrebungen staatlicher wie privatwirtschaftlicher Einrichtungen personenbezogene Daten in zentralen, vorerst noch rein nationalen, Datenbanken zu speichern, wuchs das Bedürfnis, diese bis dahin unbekannte, technisierte Form der Datenverarbeitung einer staatlichen Kontrolle zu unterwerfen.

---

[1] BG vom 18.10.1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG), BGBl 1978/565.
[2] Vgl dazu *Singer* in *Wittmann* (Hrsg), Datenschutzrecht im Unternehmen, Wien 1991.
[3] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 12; vgl dazu auch *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 182.

IdZ ist va auf das hessische Datenschutzgesetz vom 7.10.1970, GVBl. I S. 625 (das erste allgemeine Datenschutzgesetz der Welt überhaupt[4]), das französische Gesetz vom 17.7.1970 Nr 70-643 über die Garantie der bürgerlichen Rechte, das schwedische Datengesetz vom April 1973 sowie den englischen Post office Act 1969 hinzuweisen.[5]

Die Zielsetzungen des österreichischen Gesetzgebers waren bereits etwas umfassender; war in den angeführten nationalen Regelungen vorrangig noch eine strenge Kontrolle bzw Hintanhaltung einer uferlosen Datenverarbeitung mittels zentraler Datenbanken wesentliches Regelungsziel, zeichnete sich das DSG 1978 bereits durch die Schaffung von Betroffenenrechten und einer stärkeren Betonung des Gedankens der Privatsphäre aus.[6] Darüber hinaus nahm Österreich insofern eine Vorreiterrolle ein, als der Datenschutz erstmals auch eine verfassungsrechtliche Verankerung als Grundrecht erfuhr.

Wesentliche Änderungen brachte schließlich die DSG-Nov 1986[7]. Hervorzuheben ist insb die Einführung sog Standard- und Musteranwendungen[8]. Dabei handelt es sich um vordefinierte Datenverwendungen, die typischerweise in Unternehmen vorkommen wie zB die Führung einer modernen Personalverwaltung oder Buchhaltung.[9] Da in solchen Bereichen prinzipiell angenommen werden kann, dass Datenanwendungen stattfinden, wurde eine Ausnahme von der Meldepflichtigkeit solcher Datenverarbeitungen statuiert. Ziel dieser Neuerung war eine Vereinfachung des Registrierungsvorganges beim Datenverarbeitungsregister (DVR), da für diese (Standard-) Datenanwendungen forthin keine Registrierungspflicht mehr bestand. Im Bereich der Musteranwendungen ist zwar nach wie vor eine Registrierung erforderlich, eine Erleichterung für den Normunterworfenen bedeutet hier jedoch der Umstand, dass vom Erfordernis einer genauen inhaltlichen Beschreibung der Datenverarbeitung abgesehen wird.[10]

---

[4] *Gola/Schomerus*, dBDSG[9] (2007) Rz 1.
[5] Vgl dazu *Dohr/Pollirer/Weiss*, DSG (1988) 230.
[6] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 13.
[7] Bundesgesetz vom 27.06.1986 mit dem das Datenschutzgesetz und das Einführungsgesetz zu den Verwaltungsverfahrensgesetzen geändert werden (Datenschutzgesetz-Nov 1986), BGBl 1986/370.
[8] § 23 Abs 4 Datenschutzgesetz-Nov 1986.
[9] *Knyrim*, Datenschutzrecht (2003) 32.
[10] *Knyrim*, Datenschutzrecht (2003) 45.

Das DSG 1978 wies bereits einige strukturelle Merkmale des derzeit geltenden Datenschutzgesetzes 2000[11] (DSG) auf, am augenscheinlichsten darunter die Statuierung eines Grundrechts auf Geheimhaltung personenbezogener Daten im ersten Artikel des Gesetzes.[12] Weiters werden in dieser Bestimmung auch die subjektiven Rechte auf Auskunft, Richtigstellung und Löschung normiert.

Das Grundrecht auf Datenschutz gilt dabei insb auch zwischen Privaten, es kommt ihm somit unmittelbare Drittwirkung zu.[13] Dies ergibt sich insb aus der den Rechtsschutz betreffenden Kompetenzanordnung, wonach gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, das Grundrecht auf Datenschutz (mit Ausnahme des Rechts auf Auskunft) auf dem Zivilrechtsweg geltend zu machen ist.[14]

Das DSG 1978 war in seinen einfachgesetzlichen Vorschriften durch eine sehr strikte Trennung zwischen dem privaten und öffentlichen Bereich geprägt.[15] Diese Trennung wurde im DSG bis auf den Bereich des Rechtsschutzes aufgehoben, wobei wiederum als Ausnahme hiervon im privaten Bereich das Recht auf Auskunft vor der Datenschutzkommission (DSK) geltend zu machen ist.[16]

Gravierende Änderungen könnten sich nun auch durch die jüngste geplante Nov[17] zum DSG ergeben. Exemplarisch hinzuweisen ist hierbei etwa auf die Bestimmungen zur bisher nicht geregelten Videoüberwachung. Eine punktuelle Untersuchung der im Einzelnen interessierenden Fragestellungen der geplanten neuen Gesetzeslage wie auch der Kritik die diese Nov mittlerweile erfahren hat, wird an gegebener Stelle geboten.

Sowohl die Struktur als auch Entwicklung des derzeit geltenden DSG beruhen in wesentlichen Bereichen auf den diesbezüglichen gemeinschaftsrechtlichen Vorgaben. Um diese nachvollziehen zu können, wird im Anschluss eine kurze Darstellung der europarechtlichen Genese des Datenschutzrechtes geboten.

---

[11] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG), BGBl I 1999/165 idF BGBl I 2008/2.
[12] § 1 DSG.
[13] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 1 Anm 2; *Öhlinger*, Verfassungsrecht[7] (2007) Rz 833; *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 23; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 94; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 15.
[14] § 1 Abs 5 DSG; *Dohr/Pollirer/Weiss*, DSG[2] I (2002) 8.
[15] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 127;
vgl dazu auch *Knyrim*, Datenschutzrecht (2003) 11.
[16] Vgl dazu *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 24.
[17] ME DSG-Novelle 2010, 62/ME 24. GP.

2. Die europarechtliche Entwicklung des Datenschutzes und ihre Auswirkungen auf das österreichische Datenschutzrecht

Zwanzig Jahre lang war der Schutz personenbezogener Daten in Österreich durch die dafür maßgeblichen Normen des DSG 1978 bestimmt. Während dieser Zeitspanne haben sich nicht nur gravierende technologische Neuerungen im Bereich der Verwendung von personenbezogenen Daten zugetragen, auch die politische und insb wirtschaftliche Entwicklung des europäischen Raumes haben zu deutlich veränderten Anforderungen an die Ausgestaltung eines gesetzlichen Datenschutzes geführt. Eine der ersten Bestrebungen zur Harmonisierung des Datenschutzes im europäischen Raum stellte das Übereinkommen ETS 108 des Europarates vom 28.01.1981 dar.[18] Darin enthalten waren bereits materiellrechtliche Bestimmungen in Form von Grundprinzipien, besondere Vorschriften für den grenzüberschreitenden Datenverkehr sowie Regelungen betreffend das Verfahren für die gegenseitige Hilfeleistung und Konsultation zwischen den Vertragsparteien.[19]

Mittlerweile ist in der Europäischen Union praktisch jedes unternehmerische Handeln, ebenso wie die Beziehungen der Mitgliedstaaten untereinander, zwangsläufig mit der Verwendung personenbezogener Daten verbunden.[20] Die gesetzliche Regelung des Datenschutzes hat im Zuge dessen eine Verlagerung von einer nationalstaatlichen auf die gemeinschaftsrechtliche Ebene erfahren.

Art 3 Abs 1 lit c) EGV[21] schreibt als eines der grds Ziele der Gemeinschaft die Errichtung eines europäischen Binnenmarktes, der durch die Beseitigung der Hindernisse für den freien Waren-, Personen-, Dienstleistungs- und Kapitalverkehr zwischen den Mitgliedstaaten gekennzeichnet ist, fest. Auch der freie Verkehr von personenbezogenen Daten ist von dieser Zielsetzung erfasst.[22]

---

[18] Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981, BGBl 1988/317.
[19] Vgl dazu *Dohr/Pollirer/Weiss*, DSG (1988) 326.
[20] *Siemen*, Datenschutz als europäisches Grundrecht (2006) 35.
[21] Konsolidierte Fassung des Vertrages zur Gründung der Europäischen Gemeinschaft, ABl C 325 v 24.12.2002.
[22] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 65.

Die Gewährleistung eines freien Datenverkehrs in der Gemeinschaft ohne Behinderung durch nationale Grenzen, stellt sich daher iE als Voraussetzung eines europäischen Binnenmarktes dar.

Um diesen neuen Herausforderungen gerecht zu werden, wurde seitens des europäischen Gesetzgebers am 24. Oktober 1995 die Europäische Datenschutzrichtlinie[23] erlassen, deren Zweck die Harmonisierung der datenschutzrechtlichen Vorschriften der einzelnen Mitgliedstaaten der Europäischen Union ist. Zusammen mit der Datenschutzrichtlinie für elektronische Kommunikation[24] und der Datenschutzverordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[25] bildet sie das Fundament des europäischen Datenschutzes.[26]

Durch die RL 95/46/EG soll die Kommunikation personenbezogener Daten im Gemeinschaftsraum derart ermöglicht werden, dass kein Mitgliedstaat mehr den grenzüberschreitenden Datenverkehr von besonderen Prüfungen oder Genehmigungen abhängig machen darf. Die Umsetzung dieser RL hätte in Österreich bis zum 24.10.1998 geschehen sollen, tatsächlich erfolgte sie jedoch erst mit 01.01.2000.[27]

Sollten die Vorgaben der RL 95/46/EG ursprünglich durch eine Novellierung des bestehenden DSG 1978 erfolgen, entschied der Gesetzgeber schließlich, diese durch die Schaffung eines neuen Datenschutzgesetzes zu realisieren.[28] Einige wesentliche Merkmale des DSG 1978 wurden dennoch aufrechterhalten. Am augenscheinlichsten ist die Beibehaltung des Grundrechtes auf Datenschutz.[29] Dieses verfassungsgesetzlich gewährleistete Recht ist wiederum in den einfachgesetzlichen Bestimmungen des DSG bezüglich seines Inhaltes wie seiner verfahrensrechtlichen Durchsetzung in den §§ 4 bis

---

[23] Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

[24] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl L 2002/201, 37.

[25] Verordnung (EG) 45/2001 des Europäischen Parlaments und des Rates vom 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl L 2001/8, 1.

[26] Vgl *Grussmann* in *Reiter/Wittmann-Tiwald* (Hrsg), Goodbye Privacy – Grundrechte in der digitalen Welt (2008) 24.

[27] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 11.

[28] *Dohr/Pollirer/Weiss*, DSG² I (2002) 5.

[29] § 1 DSG.

64 DSG näher ausgestaltet.[30] Ebenso wie nach dem DSG 1978 bestehen auch nach dem DSG entsprechende Standard- und Musteranwendungen.[31]

Eine echtes Novum, das durch Umsetzung der RL 95/46/EG Eingang in das österreichische Datenschutzrecht fand, stellte das grds Verbot der Verwendungen sog „sensibler Daten“[32] (ein im österreichischen Datenschutzrecht bis dahin unbekannter Begriff) durch § 1 Abs 2 DSG dar.[33] Auch wurde der datenschutzrechtlich erfasste Bereich nun auf die Verwendung von Daten in manueller, strukturierter Form ausgedehnt.[34]
Die generelle Zulässigkeit einer Verarbeitung personenbezogener Daten wurde von der Einhaltung bestimmter, in § 6 DSG festgelegter, Grundsätze abhängig gemacht.[35] Diese Grundsätze waren großteils bereits im Übereinkommen ETS 108 des Europarates[36] enthalten und wurden aus diesem auch inhaltlich weitgehend übernommen.

Insb hinzuweisen ist auf das Erfordernis, dass eine Datenverarbeitung nur nach „Treu und Glauben“ erfolgen dürfe. Der genaue begriffliche Inhalt der Formulierung, die sich im identen Wortlaut[37] bereits im Übereinkommen ETS 108 findet, ist jedoch unklar. Neben der Interpretation als generellem sittlichen Grundsatz ähnlich dem Grundsatz der Übung des „redlichen Verkehrs“[38] dürfte eine Datenverwendung nach „Treu und Glauben“ va dann vorliegen, wenn der Betroffene über die Umstände des Datengebrauchs und das Bestehen bzw die Durchsetzbarkeit seiner Rechte nicht irregeführt oder im Unklaren gelassen wird.[39]

Ob eine Verarbeitung personenbezogener Daten generell zulässig ist wurde von zwei Voraussetzungen abhängig gemacht: Zum einen muss eine entsprechenden Berechtigung des Auftraggebers der Datenverarbeitung vorliegen, zum anderen sind die

---

[30] Vgl *Dohr/Pollirer/Weiss* DSG[2] I (2002) 5.
[31] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004), BGBl II 2004/312.
[32] § 4 Z 2 DSG; vgl Art 8 Abs 1 RL 95/46/EG.
[33] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 113.
[34] Art 3 iVm Art 2 lit c RL 95/46/EG; § 1 Abs 3 DSG; mwN *Dohr/Pollirer/Weiss* DSG² I (2002) 5.
[35] Vgl *Dohr/Pollirer/Weiss*, DSG² I (2002) 6.
[36] Vgl Art 5 des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981.
[37] Art 5 lit a des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981.
[38] *Knyrim*, Datenschutzrecht (2003) 82.
[39] Vgl ErläutRV 1613 BlgNR 20. GP 39.

schutzwürdigen Interessen der Betroffenen zu berücksichtigen.[40] Dies wurde in den §§ 6, 7, 8 und 9 DSG umgesetzt. Der österreichische Gesetzgeber hat hierbei jedoch ein verhältnismäßig kompliziertes System von Verweisen geschaffen, was weiter zu den bereits erwähnten Schwierigkeiten bei der Verständlichkeit der Normen beitrug.[41]

Da die RL 95/46/EG als zentrales Anliegen die Gewährleistung eines freien Datenverkehrs am europäischen Binnenmarkt bezweckt, stellt sich in diesem Zusammenhang auch die Frage nach der Zulässigkeit des Datenverkehrs mit Drittländern (d.h. Staaten außerhalb des EU- bzw EWR-Gebiets). Ein solcher Datenverkehr ist nach den gemeinschaftsrechtlichen Bestimmungen nur zulässig, wenn in diesen Drittländern ein angemessenes Schutzniveau garantiert ist.[42] Von diesem grds Prinzip nicht erfasst ist jedoch der Bereich der sog „dritten Säule“ der EU - die Zusammenarbeit der EU-Mitgliedstaaten in den Sektoren Justiz und Inneres - da die RL 95/46/EG auf diese Bereiche keine Anwendung findet.[43] Diesen gemeinschaftsrechtlichen Vorgaben wurde im österreichischen DSG durch die Bestimmungen der §§ 12 und 13 DSG entsprochen.

Schließlich wurden durch die RL 95/46/EG, dem Trend zur Stärkung des Rechts auf „informationelle Selbstbestimmung“[44] (ausgehend von einem Urteil des deutschen Bundesverfassungsgerichtshof zum deutschen Volkszählungsgesetz[45]) folgend, die Rechte der von einer Datenverarbeitung Betroffenen gestärkt. So wurde insb mit der Bestimmung des § 28 DSG ein Recht auf Widerspruch des Betroffen gegen die Verwendung seiner Daten bei Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen beim Auftraggeber der Datenanwendung implementiert.[46]

---

[40] Art 7 RL 95/46/EG.
[41] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 21.
[42] Art 25 RL 95/46/EG; zur Bedeutung des Übereinkommen ETS 108 des Europarates in diesem Zusammenhang vgl *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 275.
[43] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 154.
[44] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 13; vgl dazu auch *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 182.
[45] Gegenstand der Entscheidung waren die im Zuge der Volkszählung 1983 erhobenen personenbezogenen Daten; BVfG 15.12.1983, BVfGE 65, 1 = NJW 1984, 419 = EuGRZ 1983, 577; mwN *Simitis*, dBDSG[6] (2006) 73; *Gola/Schomerus*, dBDSG[9] (2007) § 1 Rz 12.
[46] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 110; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 218; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 106; *Knyrim*, Datenschutzrecht (2003) 227; vgl Art 14 RL 95/46/EG; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 82.

II. Der durch das DSG geschützte Personenkreis

§ 1 DSG statuiert einen Anspruch auf Geheimhaltung personenbezogener Daten. Darunter sind der Schutz des Betroffenen vor Ermittlung seiner Daten und der Schutz vor der Weitergabe der über ihn ermittelten Daten zu verstehen.[47] Fraglich ist nun, wer als Betroffener iSd Formulierung und somit als Träger dieses Grundrechts in Betracht kommt.

A. Natürliche und juristische Personen

Nach der geltenden Rechtslage sind vom datenschutzrechtlichen Begriff des Betroffenen nicht nur natürliche Personen sondern auch juristische Personen und Personengemeinschaften erfasst.[48] Österreich gehört somit zu einem der wenigen EU-Mitgliedsstaaten (wie zB Italien und Dänemark), in denen der Datenschutz nicht auf natürliche Personen beschränkt ist.[49] Dies ist insofern bewerkenswert, als der österreichische Gesetzgeber den Schutz personenbezogener Daten dadurch weitgehender garantiert hat, als das aufgrund der gemeinschaftsrechtlichen Anforderungen notwendig gewesen wäre.[50]

Es besteht daher iE auch für juristische Personen ein verfassungsgesetzlich gewährleisteter Schutz ihrer personenbezogenen Daten, sofern das Grundrecht in derartigen Fällen zur Anwendung kommen kann.[51]

Grundrechtsträger ist immer der Betroffene im Sinne von § 4 Z 3 DSG (der Legaldefinition zufolge jede vom Auftrageber der Datenanwendung verschiedene natürliche oder juristische Person oder Personengemeinschaft deren Daten verwendet

---

[47] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 1 Anm 2.
[48] § 4 Z 3 DSG.
[49] *Knyrim*, Datenschutzrecht (2003) 11; vgl RL 95/46/EG ErwG 24.
[50] ErwG 24 und Art 1 Abs 1 RL 95/46/EG; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 109; jedoch kann für juristische Personen in Staaten von deren datenschutzrechtlichen Vorschriften sie nicht erfasst sind insofern eine Geltendmachung datenschutzrechtlicher Ansprüche in Betracht kommen, als sich diese aus einem allgemein (auch für juristische Personen geltenden) Persönlichkeitsrecht ableiten lassen; vgl idZ *Gola/Schomerus*, dBDSG[9] (2007) § 3 Rz 11.
[51] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 5; so kann bei juristischen Personen etwa ein Schutz sensibler Daten gar nicht in Betracht kommen, da diese Art personenbezogener Daten nur bei natürlichen Personen gegeben ist.

werden)[52]. Dieser ist Adressat der gewährleisteten Rechte, wie des Rechts auf Geheimhaltung, des Informationsrechts sowie sonstiger Betroffen-Rechte.[53] Der durch das DSG geschützte Personenkreis setzt sich iE somit aus natürlichen und juristischen Personen jedweder Organisationsform zusammen.

B. Das Unternehmen als juristische Person

Klärungsbedürftig ist zunächst, was unter dem Begriff des „Unternehmens" zu verstehen ist: Als Erscheinungsform im wirtschaftlichen Alltag kann das Unternehmen als eine Organisation beschrieben werden, die den Zweck verfolgt, auf dem Markt wirtschaftlich werthafte Leistungen gegen Entgelt anzubieten.[54] Eine Legaldefinition bieten va § 1 Abs 2 KSchG[55] sowie § 1 Abs 2 UGB[56] (der wiederum an die Definition des KSchG anknüpft)[57] wonach ein Unternehmen jede auf Dauer angelegte Organisation selbständiger wirtschaftlicher Tätigkeit ist, mag diese auch nicht auf Gewinn ausgerichtet sein.

Auf der Ebene der rechtlichen Qualifikation ist aus diesen Definitionen jedoch noch nichts gewonnen. Das Unternehmen an sich stellt noch keine juristische Person dar (und kann für sich somit auch nicht Betroffener iSd § 4 Z 3 DSG sein), zur Abklärung der konkreten Rechtsfähigkeit muss notwendigerweise auf den jeweiligen Unternehmensträger abgestellt werden.[58]

Unter den von der Rechtsordnung diesbezüglich zur Verfügung gestellten Einrichtungen bevorzugen Unternehmen oftmals eine Konstruktion in Form der Gesellschaft. Diese stellt sich idR als eine durch Rechtsgeschäft begründete Rechtsgemeinschaft zweier oder mehrerer Personen, um einen gemeinsamen Zweck mit gemeinsamen Mitteln zu

---

[52] Zu den Begriffen Auftraggeber, Datenanwendung und Verwenden von Daten vgl die Legaldefinitionen des § 4 Z 4,7 und 8 DSG.
[53] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 28.
[54] *Krejci*, Unternehmensrecht[4] (2008) 34; mwN *Rauter*, Unternehmen, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) 316.
[55] Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffenen werden (Konsumentenschutzgesetz – KSchG) BGBL 1979/140 idF BGBl I 2008/21.
[56] Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgesetzbuch – UGB) dRGBl S 219/1897 idF BGBl I 2008/70.
[57] *Schummer/Kriwanek*, Das neue Unternehmensgesetzbuch (2006) Anm zu § 1 UGB; vgl dazu auch *Zib* in *Zib/Verweijen* (Hrsg), Das neue Unternehmensgesetzbuch (2006) § 1 Anm 1.
[58] *Beisel/Klumpp*, Unternehmenskauf[5] (2006) 1. Kap Rz 22.

erreichen dar.[59] Eine aus der modernen Marktwirtschaft nicht mehr wegzudenkende Organisationsform stellen insb Kapitalgesellschaften dar.

Sowohl die Gesellschaft mit beschränkter Haftung (GmbH) als auch die Aktiengesellschaft (AG) haben sich besonders bei Unternehmen mit großem Umsatz und internationaler Ausrichtung als eine der am häufigsten gewählten Rechtsformen bewährt. GmbH und AG sind als Kapitalgesellschaften dem Gesetz (§ 61 Abs 1 GmbHG[60], § 1 AktG[61]) nach mit eigener Rechtspersönlichkeit ausgestattet und somit ex lege juristische Personen.[62] Als solche sind sie Träger des Grundrechts auf Datenschutz und genießen in Folge auch sämtliche daraus erfließenden Betroffenenrechte.

Der Umstand, dass im Ergebnis somit sowohl die GmbH als auch die AG unter den Betroffenenbegriff des § 4 Z 3 DSG zu subsumieren ist, hat insb für den Bereich der gesellschaftsrechtlichen Umstrukturierungen eine ganz wesentliche Bedeutung: Die Vorschriften des Datenschutzrechts bei Verschmelzungen, Umwandlungen und Spaltungen können daher nicht nur bezüglich der dabei verwendeten Daten natürlicher Personen, sondern auch in Hinsicht auf die Wirtschafts- und Unternehmensdaten der bei der Umstrukturierung involvierten Gesellschaften selbst beachtlich sein.

[59] Vgl *Mader*, Kapitalgesellschaften[6] (2008) 1.
[60] Gesetz vom 6. März 1906, über Gesellschaften mit beschränkter Haftung (GmbH-Gesetz – GmbHG), RGBl 58/1906.
[61] Bundesgesetz vom 31. März über Aktiengesellschaften (Aktiengesetz 1965), BGBl 1965/98 idF BGBl I 2008/70.
[62] Vgl dazu *Jabornegg* in *Jabornegg/Strasser* (Hrsg) AktG[4] (2006) § 1 Rz 17.

III. Grundsätzliche Überlegungen zum Datenschutz im Unternehmen

Datenschutz im Unternehmen stellt sich als eine Vielzahl von Anforderungen dar, um den Schutz personenbezogener Daten innerhalb der unterschiedlichen Rechtsbeziehungen gegenüber den einzelnen Gruppen von Betroffenen gewährleisten zu können.[63] Um den Schutz personenbezogener Daten sicherzustellen, müssen die in Betracht kommenden kritischen Abläufe im Unternehmen auf mehreren Ebenen den gesetzlichen Vorgaben entsprechend gestaltet werden: Dies erfordert ebenso die Schaffung rein technisch-organisatorischer Strukturen wie auch ein Verfahren zur wirksamen Vorabkotrolle der rechtlichen Zulässigkeit von Datenverarbeitungen.[64]

Eine in der Praxis für Unternehmen schwierige Entwicklung der letzten Jahre stellt der Umstand dar, dass in manchen Bereichen des Geschäftsalltags eine klare Zuordnung der Verantwortlichkeit für die Sicherstellung des Datenschutzes oftmals auf den ersten Blick nicht eindeutig erkennbar scheint.

Dies liegt va in den wirtschaftlichen Mechanismen der modernen Informationsgesellschaft begründet. So ist es bspw bei vielen Unternehmen der Konsumartikelsparte Usus zwecks Kundenbindung entsprechende Kundenkarten auszugeben. Die Entscheidung in welchem Umfang hierbei Informationen vom Konsumenten bereitgestellt werden kann im Rahmen der subjektiven Verantwortung nur von diesem selbst getroffen werden.

Somit kommt auch dem Vertragspartner des Unternehmens als Betroffenem zunehmend eine aktive Rolle beim Schutz der ihn betreffenden personenbezogenen Daten zu. Hinzuweisen ist idZ auf das Widerspruchsrecht nach § 28 Abs 1 DSG, das auf spezielle in der Person des Betroffenen liegende Gründe abstellt, die dem Unternehmen typischerweise nicht bekannt sind und von diesem daher auch nicht berücksichtigt werden können.[65]

---

[63] *Wächter*, Datenschutz im Unternehmen (2003) 5.
[64] Vgl dazu die diesbezüglichen Vorgaben der §§ 6, 7, 8, 9 und 14 DSG.
[65] ErläutRV 1613 BlgNR 20. GP 48; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 106; *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 111; *Graf*, Datenschutzrecht im Überblick, 73.

Bei den im Unternehmen selbst bestehenden datenschutzrechtlich beachtlichen Beziehungen ergeben sich insb im Bereich von Arbeitsverhältnissen Fragestellungen. Durch die moderne Informationstechnologie stellen sich Fragen bei der Ausgestaltung von Personalinformations- und Kontrollsystemen durch das Unternehmen in seiner Rolle als Arbeitgeber sowie auch bei der Nutzung von Informationssystemen durch die Arbeiternehmer selbst.[66]

Da das Grundrecht auf Datenschutz weiters ebenso Wirtschaftsdaten als auch personenbezogene Daten[67] einer juristischen Person umfasst, sind die maßgeblichen Vorschriften des DSG neben dem Umgang mit vertraulichen Informationen über Kunden und Lieferanten auch im Hinblick auf den Schutz von Betriebsgeheimnissen zu beachten.

Nicht zu vernachlässigen sind schließlich auch die Konsequenzen, die eine Missachtung der datenschutzrechtlichen Vorgaben nach sich ziehen kann. Diese können von einer gerichtlichen Freiheitsstrafe bis zur Verhängung einer Verwaltungsstrafe von bis zu € 18.890,-- reichen.[68] Für das Unternehmen in der Praxis uU noch gravierender als etwaige Strafen wird dabei insb die zu befürchtende negative Publicity sein. Der Imageverlust, der aus dem Bekanntwerden resultiert, dass ein bestimmtes Unternehmen datenschutzrechtliche Vorschriften nicht oder nicht ausreichend erfüllt, kann sich leicht auf dessen Umsätze auswirken und somit einen nicht unerheblichen wirtschaftlichen Schaden verursachen.[69]

Zusammenfassend geht es daher heute beim Schutz personenbezogener Daten im Unternehmen insb um den Schutz von Unternehmenswerten, den Schutz der Unternehmensprozesse, die Sicherheit für Kunden, Lieferanten, Partner und Mitarbeiter sowie die Gewährleistung einer entsprechend datenschutzkonformen Organisation an sich.[70]

---

[66] Vgl *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)*, Geheimnisschutz-Informationsschutz-Datenschutz (2008) 288.

[67] § 4 Z 1 DSG; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 26; vgl VfGH 30.11.1989, Slg 12.228.

[68] §§ 51 Abs 1 und 52 Abs 1 DSG.

[69] *Knyrim*, Datenschutzrecht (2003) 245.

[70] *Wächter*, Datenschutz im Unternehmen (2003) 23.

A. Neue Schutzbedürftigkeit der Betroffenen

Mit der rasanten Entwicklung der automationsunterstützten Datenverarbeitung in der Wirtschaft und nicht zuletzt auch in vielen Bereichen des modernen Sozialstaates steigt auch die Schutzbedürftigkeit der solchen Verarbeitungen Unterworfenen. Sei es als Kunde eines Unternehmens, als Arbeitnehmer oder Steuerzahler, der Betroffene steht in einer Vielzahl von Rechtsbeziehungen, die eine umfangreiche Datenerhebung, -verarbeitung und -nutzung seiner personenbezogenen Daten mit sich bringen.

Geschäftliche wie private Beziehungen leben davon, dass Informationen ausgetauscht werden. Es ist dem Einzelnen im modernen Sozialstaat nahezu unmöglich geworden, die Informationsbedürfnisse anderer abzuwehren ohne sich selbst von praktisch allen beruflichen wie sozialen Abläufen zu isolieren.[71] Hinzu kommt, dass bei den Betroffenen in den seltensten Fällen ein entsprechendes Problembewusstsein sowohl bei der Zurverfügungstellung personenbezogener Daten als auch bei den zur Sammlung solcher Daten geeigneten Lebenssachverhalten vorhanden ist.

So kann bereits die Nutzung einer einfachen Internet-Suchmaschine zur Preisgabe einer Vielzahl von Informationen über den Benutzer führen.[72] Als nicht minder problematisch erweist sich besonders iZm Internet-Archiven (oder auch sozialen Netzwerken)[73] der Umstand, dass einmal preisgegebene personenbezogene Daten zeitlich nahezu unbegrenzt verfügbar sind. Eine Löschung dieser Daten kann sich dann oftmals als praktisch unmöglich erweisen; bewusst ist dies freilich den Wenigsten.[74]

---

[71] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 13; vgl dazu auch *Holaschke*, Einflussfaktoren auf die Bereitschaft personenbezogene Daten zur Verfügung zu stellen (2007) 10.

[72] http://www2.argedaten.at/session/anonym242093opojia972491.E42_INP.html (20.10.2008); zur grds Problematik von Suchmaschinen s *Weichert*, Datenschutz bei Suchmaschinen, MR-Int 2007, 188; vgl dazu auch *Settele*, Das Schlüsselloch Internet - Suchmaschine serviert Personendaten, Neue Zürcher Zeitung vom 5.2.2008.

[73] Vgl *Spiegler/Kocina*, Ich lass dich nie mehr allein…, Die Presse vom 29.1.2009; vgl dazu auch Übereifrige Datensammler in Vorarlberg – AK fordert schärfere Datenschutzgesetze, Artikel auf ORF.at vom 28.4.2009 (http://vorarlberg.orf.at/stories/358395); s idZ auch *Art 29 Datenschutzgruppe*, Stellungnahme 5/2009 zu Online-Social-Networking, http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_25_06_09_en.pdf (1.7.2009).

[74] *Mayer-Schönberger* in *Reiter/Wittmann-Tiwald* (Hrsg), Goodbye Privacy – Grundrechte in der digitalen Welt (2008) 9; vgl dazu weiters *Reischl*, Striptease am Daten-Highway, Kurier vom 5.10.2008.

B. Neue Wirtschaftsmechanismen

Im Zuge der weltweiten Verbreitung des Internets entstand für Unternehmen die Möglichkeit Informationen, Dienstleistungen und Waren direkt an den Kunden zu bringen (B2C)[75]. Es ist für diesen nicht selten Voraussetzung sich durch seine persönlichen Daten registrieren zu müssen, bevor er überhaupt Dienste solcher Unternehmen in Anspruch nehmen kann.

Im Bereich des E-Commerce stellt sich die Herausgabe persönlicher Daten als geradezu alltäglich dar.[76] Durch deren Auswertung lassen sich ebenso Informationen über Konsumgewohnheiten und Bonität, wie auch zielführende Maßnahmen zur Bindung bestehender sowie Akquirierung neuer Kunden gewinnen.[77] Unternehmen können sich somit bereits allein durch Sammlung und effiziente Nutzung personenbezogener Daten einen Wettbewerbsvorteil verschaffen; entsprechende Datenbanken haben daher einen nicht zu unterschätzenden Einfluss auf den Unternehmenserfolg.[78]

Gerade Werbeagenturen, Adressverlage und Direktmarketingunternehmen haben als datenverarbeitende Stelle häufig überhaupt keine direkte Beziehung mehr zu den Betroffen, sondern beziehen deren Daten überwiegend aus anderen Quellen.[79] All diese Entwicklungen tragen dazu bei, dass personenbezogene Daten zunehmend selbst zum teuer gehandelten (ohne dass jedoch die jeweiligen Betroffenen selbst davon profitieren) Wirtschaftsgut werden.[80]

Aber auch auf anderen Gebieten haben sich durch den rasanten technologischen Fortschritt der letzten Jahre datenschutzrechtlich bedenkliche Konstellationen ergeben: Hinzuweisen ist idZ etwa auf sog RFID-Chips (Radio Frequency Identification), als

---

[75] B2C ist der englische, auch in der d Sprache gebräuchliche, Ausdruck für den elektronischen Geschäftsverkehr zwischen Unternehmen und Verbraucher; *Fina*, B2C, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) 33; vgl dazu auch *Kramer/Herrmann*, Datenschutz und E-Commerce (2005) 14 Rz 6.

[76] *Wächter*, Datenschutz im Unternehmen (2003) 66.

[77] *Kramer/Herrmann*, Datenschutz und E-Commerce (2005) 17; mwN *Patzak*, Datenschutzrecht für den E-Commerce (2006) 35.

[78] *Holaschke*, Einflussfaktoren auf die Bereitschaft personenbezogene Daten zur Verfügung zu stellen (2007) 4.

[79] *Wächter*, Datenschutz im Unternehmen (2003) 257.

[80] Vgl zu dieser Entwicklung auch Neue Hürden für Datenhändler, Artikel auf ORF.at vom 10.12.2008 (http://futurezone.orf.at/stories/1500676/); Brisantes Datenleck in Deutschland, Artikel auf ORF.at vom 13.12.2008 (http://orf.at/081213-32774/index.html).

Nachfolger der herkömmlichen Strichcodes, zur Kennzeichnung von Waren.[81] Im Gegensatz zu Strichcodes können diese Chips kontaktlos, und iE ohne Wissen des Trägers, über Funk ausgelesen werden. Die verschiedenen Einsatzmöglichkeiten sind aus datenschutzrechtlicher Sicht jedenfalls nicht unbedenklich.[82]

Wird zwar zumeist nicht der Name einer Person gespeichert, sondern nur eine Nummer, könnte man doch einer Person eine große Menge Daten zuordnen, mag diese dem "Ausleser" namentlich auch unbekannt sein. Sofern diese Daten nicht anonym sind, sind datenschutzrechtliche Implikationen durchaus denkbar.[83]

[81] *Hödl*, Die Macht der klugen Dinge, Überlegungen zu ubiquitous computing, RFID-Chips und smart objects, juridikum 2007, 210.
[82] Vgl dazu *Gola/Schomerus*, dBDSG[9] (2007) § 6 c Rz 5a.
[83] *Knyrim/Haidinger*, RFID-Chips und Datenschutz, RdW 2005, 1b.

C. Datenschutzrechtliche Anforderungen an die Verwendung personenbezogener Daten durch Unternehmen

Einen für Unternehmen in der Praxis äußerst bedeutsamen Umstand stellt auch die grds Meldepflichtigkeit jeder Datenanwendung[84] dar; diese ist in § 17 DSG geregelt.

Aus der in Abs 1 S 1 der Bestimmung enthaltenen Formulierung[85] folgt als Grundregel, dass jeder, der eine Datenverarbeitung betreiben möchte, diese vor ihrer Aufnahme melden muss; dies gilt ebenso für jede Änderung oder Ergänzung einer bereits registrierten Datenanwendung (s auch § 4 Z 3 DVRV 2002). Für Unternehmen bedeutet dies iE, dass sie ihre Meldungen beim DVR stets aktuell zu halten haben.[86]

1. Vereinfachung durch Standard- und Musteranwendungen

Eine in der unternehmerischen Praxis bedeutsame Ausnahme von der Meldepflicht enthält dafür § 17 Abs 2 Z 6 DSG: Solche Datenverarbeitungen, die im wirtschaftlichen Alltag selbstverständlich und notwendig sind, wie zB Lohnverrechnung, Buchhaltung sowie Kunden- und Lieferantendateien, sind in entsprechenden Standardanwendungen[87] erfasst. Entspricht die Datenverarbeitung einer Standardanwendung, muss die Verarbeitung nicht beim DVR gemeldet werden, was für viele Unternehmen eine erhebliche Erleichterung bedeutet.

Als weitere Ausnahmen von der Meldepflicht sind in § 17 Abs 2 DSG bspw veröffentlichte, nur indirekt personenbezogene Daten oder Daten, die für rein private[88] oder publizistische Zwecke[89] verwendet werden normiert. § 17 Abs 3 DSG enthält schließlich Datenverarbeitungen iZm Interessen aus dem Gesichtspunkt der

---

[84] § 4 Z 8; leg cit, die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

[85] § 17 Abs 1 S 1 DSG; leg cit, Jeder Auftraggeber hat, soweit in den Abs 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten.

[86] *Knyrim*, Datenschutzrecht (2003) 177; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 177.

[87] Derzeit sind 31 Standardanwendungen erfasst; s Anlage 1 StMV 2004.

[88] § 45 DSG; zum Umfang der Zulässigkeit einer Datenverwendung für private Zwecke s bspw EuGH 6.11.2003, C-101/01, *Lindqvist*, Slg 2003, I-12971.

[89] § 48 DSG.

„Staatssicherheit“, so zB Verarbeitungen zur Landesverteidigung oder zur Strafverfolgung, wobei hier von einer näheren Untersuchung abgesehen wird, da diese Fälle für Unternehmen als private Datenverarbeiter kaum beachtlich sein werden.[90]

Nach § 19 Abs 2 DSG besteht weiters die Möglichkeit, dass, wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen haben und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, der Bundeskanzler durch V Musteranwendungen festlegen kann.[91] Entspricht die Datenverarbeitung einer Musteranwendung, besteht zwar nach wie vor die Pflicht zur Meldung beim DVR, als Vereinfachung muss jedoch nur die Tatsache des Vorliegens der Musteranwendung selbst und nicht deren jeweiliger genauer Inhalt gemeldet werden.

Für Unternehmen ebenfalls beachtlich ist die Pflicht zur Information der von der Datenanwendung Betroffenen über Zweck und Identität des datenschutzrechtlichen Auftraggebers gem § 24 DSG. Diese soll es dem Betroffenen erleichtern, seine Rechte zu wahren.[92] Von der Informationspflicht ausgenommen sind dafür Standardanwendungen.[93]

2. Genehmigungspflichtiger Datenexport

An dieser Stelle kurz angesprochen seien auch jene Fälle in denen es zu einer Übermittlung personenbezogener Daten ins Ausland kommt. Maßgeblich idZ sind die Bestimmungen der §§ 12 u 13 DSG.

Insb bei grenzüberschreitenden Umstrukturierungen sowie in Konzernstrukturen kommt es regelmäßig zu derartigen Übermittlungen. Finden diese innerhalb der EU bzw des EWR statt, stellen sie sich grds unproblematisch dar, bei einer Übermittlung in Drittländer ohne angemessenes Schutzniveau können jedoch mitunter aufwendige Genehmigungsverfahren vor der DSK zu durchlaufen sein.

---

[90] Vgl dazu auch *Knyrim*, Datenschutzrecht (2003) 32.
[91] *Knyrim*, Datenschutzrecht (2003) 45.
[92] ErläutRV 1613 BlgNR 20. GP 45 (46); eine entsprechende Information des Betroffenen wird schon aus dem Gebot einer Datenverwendung nach Treu und Glauben folgen.
[93] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 24 Anm 4.

Aufgrund der besonderen Relevanz dieser Fragestellungen iZm Umstrukturierungen und Konzernstrukturen findet die Untersuchung der interessierenden Probleme in den entsprechenden Kap statt.[94]

Unternehmen werden jedenfalls gut beraten sein, eine entsprechende interne Organisation zur Wahrnehmung der Melde- und Genehmigungspflichten zu schaffen, da eine Missachtung letzterer, abgesehen von negativer Publicity, nicht zuletzt auch zu einer Verwaltungsstrafe führen kann.[95]

[94] S Kap V. u VI.
[95] Vgl § 52 Abs 2 Z 1 DSG.

IV. Gesetzliche Grundlagen für den Datenschutz im Unternehmen

Im Folgenden wird ein Überblick über die im unternehmerischen Alltag beachtlichen Bestimmungen zum Schutz personenbezogener Daten gegeben. Dabei zeigt sich, dass die Bestimmungen zum Datenschutz in engem Zusammenhang mit allen Erscheinungsformen moderner Informations- und Datenverarbeitung und damit auch unter dem permanenten Einfluss dynamischer Unternehmensprozesse stehen.

Ebenso zahlreich wie die für einen effektiven Datenschutz beachtlichen rechtlichen Szenarien des Geschäftsalltags (zB der Umgang mit Daten aus dem Kunden- und Lieferantenverkehr, die Wahrung von Geschäfts- und Betriebsgeheimnissen) sind auch die dafür jeweils bestehenden gesetzlichen Regelungsmaterien. [96]

Neben den Vorschriften der § 1 DSG und Art 8 EMRK[97], die im Verfassungsrang stehen, finden sich unter anderem im ABGB[98], im GmbHG[99], im AktG[100], im UWG[101], im StGB[102], im MedienG[103], im BWG[104], in der GewO[105] sowie im WTBG[106] einfachgesetzliche Bestimmungen zum Schutz (personenbezogener) Daten.

---

[96] *Wächter*, Datenschutz im Unternehmen (2003) 1.

[97] Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 1958/210 idF BGBl III 2002/179.

[98] Allgemeines bürgerliches Gesetzbuch vom 1. Juni 1811 (ABGB), JGS 1811/946 idF BGBl I 2008/100.

[99] Gesetz vom 6. März 1906, über Gesellschaften mit beschränkter Haftung (GmbH-Gesetz – GmbHG), RGBl 1906/58 idF BGBl I 2008/70.

[100] Bundesgesetz vom 31. März über Aktiengesellschaften (Aktiengesetz 1965), BGBl 1965/98 idF BGBl I 2008/70.

[101] Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG, BGBl 1984/448 idF BGBl I 2007/79.

[102] Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 1974/60 idF BGBl I 2007/112.

[103] Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz - MedienG), BGBl 1981/314 idF BGBl I 2007/112.

[104] Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG), BGBl 1993/532 idF BGBl I 2008/136; auch § 38 BWG steht im Verfassungsrang, doch wird die Abhandlung der Bestimmung aus systematischen Überlegungen dennoch in Kap IV.B. vorgenommen.

[105] Gewerbeordnung 1994 – GewO 1994, BGBl 1994/194 idF BGBl I 2008/68.

[106] Bundesgesetz über die Wirtschaftstreuhandberufe (Wirtschaftstreuhandberufsgesetz – WTBG), BGBl 1999/58 idF BGBl I 2008/10.

A. Verfassungsrechtliche Grundlagen

1. Der Schutz personenbezogener Daten durch § 1 DSG

Die Verfassungsbestimmung des § 1 DSG ist die zentrale Norm des gesetzlichen Schutzes personenbezogener Daten. Bei Vorliegen schutzwürdiger Interessen gewährt sie jedermann ein Grundrecht auf Datenschutz, wobei in Österreich (als einem der wenigen Länder im EU- und EWR-Raum mit einer solch weiten Ausgestaltung des Schutzbereiches) von diesem Recht auch juristische Personen und Personengemeinschaften erfasst sind.[107]

a) Das Grundrecht auf Geheimhaltung gem § 1 Abs 1 DSG

Im Vordergrund steht hierbei der Anspruch auf Geheimhaltung nach § 1 Abs 1 DSG, darunter ist nicht nur die unbefugte Offenlegung und sonstige Weitergabe personenbezogener Daten zu verstehen, sondern jede Art und Weise der Datenverwendung, es besteht insb ein genereller Anspruch auf Ermittlungsschutz.[108] Dieser richtet sich schon gegen die bloße Erhebung von Daten, einschließlich Verpflichtungen, nach denen solche Daten bekanntzugeben sind (zB gesetzliche Meldepflichten).

Derartige Verpflichtungen des Betroffenen sind daher immer als Eingriffe in das Grundrecht auf Datenschutz zu verstehen, die somit den dafür geltenden Voraussetzungen entsprechen müssen. Das Grundrecht auf Datenschutz steht iE daher unter einem materiellen Gesetzesvorbehalt.[109]

Voraussetzung des Geheimhaltungsanspruchs ist stets das Vorliegen eines Interesses an der Geheimhaltung, wobei als unabdingbares Erfordernis auch eine, im Einzelfall zu beurteilende, Schutzwürdigkeit dieses Interesses gegeben sein muss.[110]

---

[107] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 15.
[108] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 2; *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 64; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 12.
[109] *Öhlinger*, Verfassungsrecht[7] (2007) Rz 830; *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 10.
[110] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 7; dagegen *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 15 Rz 16.

Kein schutzwürdiges Interesse liegt gemäß § 1 Abs 1 2. S DSG bei allgemeiner Verfügbarkeit oder mangelnder Rückführbarkeit der Daten auf den Betroffenen vor.[111] Während im ersten Fall offenkundig keine Möglichkeit einer Geheimhaltung (mehr) besteht, kommt im zweiten Fall kein Anspruch des Betroffenen auf Geheimhaltung in Betracht, da gar kein Personenbezug iSd DSG besteht.

b) Einschränkungsmöglichkeiten - § 1 Abs 2 DSG

§ 1 Abs 2 DSG normiert die Voraussetzungen für die Zulässigkeit einer Beschränkung des Grundrechts auf Datenschutz. Dabei wird in der Bestimmung selbst[112] explizit der generelle Grundsatz angeführt, wonach alle Grundrechtseingriffe jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden dürfen.[113] Dies stellt iE eine verfassungsrechtliche Verankerung des nach Jud und Grundrechtsdogmatik bestehenden Verhältnismäßigkeitgebotes für das Grundrecht auf Datenschutz dar.[114]

Dem datenschutzrechtlichen Prinzip der Selbstbestimmung zufolge kann zunächst einmal die persönliche Interessenlage des Betroffenen selbst eine Beschränkung (bis hin zur völligen Aufhebung) des Geheimhaltungsanspruches rechtfertigen.[115] So muss die Verwendung seiner personenbezogenen Daten für den Betroffenen entweder lebenswichtig sein oder seine persönliche Zustimmung (wobei diese, solange sie keine sensiblen Daten betrifft, wohl auch konkludent erfolgen kann)[116] dazu vorliegen.[117]

Gerade im unternehmerischen Bereich stellt sich die Zustimmung des Betroffenen als häufiger Rechtfertigungsgrund für die Verarbeitung personenbezogener Daten dar, umso sorgfältiger ist deren tatsächliches Vorliegen zu prüfen. [118]

---

[111] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 23; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 12.
[112] § 1 Abs 2 letzter Satz DSG.
[113] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 14; vgl zur inhaltlich kongruenten Interessensabwägung schon nach dem DSG 1978 zB OGH 12.3.1997, 6 Ob 2228/96 g.
[114] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 20.
[115] *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 35 Rz 44.
[116] IdS *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 12; *Knyrim*, Datenschutzrecht (2003) 166; krit zur konkludenten Zustimmung dagegen auch bei nicht-sensiblen Daten *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 206.
[117] § 1 Abs 2 1. Satz DSG; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 15.
[118] Vgl *Knyrim*, Datenschutzrecht (2003) 159.

Als weitere zulässige Grundrechtsbeschränkung führt § 1 Abs 2 DSG schließlich überwiegende berechtigte Interessen eines anderen an. Diese müssen sich aus dem Recht bzw der Gesamtrechtsordnung ableiten lassen.[119]
Soll ein Eingriff in das Grundrecht durch eine staatliche Behörde erfolgen, kann ein Überwiegen der Eingriffsinteressen nur dann gegeben sein, wenn der Eingriff aus einem der in Art 8 Abs 2 EMRK genannten Gründe notwendig und verhältnismäßig ist.[120]

Bei einem Eingriff durch Private gibt § 1 Abs DSG dagegen keine näheren Parameter zur Abklärung, wann überwiegende berechtigte Interessen anderer vorliegen, diesbezüglich müssen die einfachgesetzlichen Ausführungsbestimmungen des DSG herangezogen werden.[121] Wirtschaftliche Interessen kommen in diesem Zusammenhang nur in Betracht, wenn sie von der Rechtsordnung auch zu berechtigten gemacht werden.[122]

Eine verfassungsrechtliche Verankerung solcher Interessen ist dabei als Indiz für das Überwiegen der Interessen anzusehen. So kann zB das Grundrecht auf Informationsfreiheit (Art 10 EMRK) bei der Interessensabwägung im Hinblick auf Personen des öffentlichen Lebens zu einem Überwiegen und damit zu einer Durchbrechung des Geheimhaltungsanspruchs führen.[123] Zusätzliche Kriterien für die Interessensabwägung ergeben sich schließlich aus dem DSG selbst.[124]

c) Rechte auf Auskunft, Richtigstellung und Löschung gem § 1 Abs 3 DSG

Weiters werden dem Betroffenen durch § 1 Abs 3 DSG Leistungsansprüche auf Auskunft, Richtigstellung und Löschung seiner personenbezogenen Daten gegeben. Diese Ansprüche sind somit ebenfalls vom Grundrecht erfasst (ein Umstand, der bereits nach der Rechtslage nach dem DSG 1978 unzweifelhaft war)[125]. Auch für diese Rechte ist jedoch der materielle Gesetzesvorbehalt des § 1 Abs 2 DSG zu beachten.[126]

---

[119] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 13.
[120] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 65.
[121] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 13.
[122] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 13.
[123] *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG, in FS Schäffer (2006) 332.
[124] Vgl dazu die §§ 6 DSG ff.
[125] VfGH G 238/88 VfSlg 12.194.
[126] Vgl § 1 Abs 4 DSG der auf §1 Abs 2 DSG verweist.

§ 1 Abs 3 DSG gibt dem Betroffenen die Möglichkeit seinen Anspruch auf Geheimhaltung durch die entsprechenden Kontroll-, Abwehr- und Gestaltungsrechte auch tatsächlich durchzusetzen zu können. Die Verbindung dieser Ansprüche mit den zu ihrer Ausführung ergangenen einfachgesetzlichen Bestimmungen verwirklichen damit das Konzept der „informationellen Selbstbestimmung“[127] auch in der österreichischen Rechtsordnung.

d) Die unmittelbare Drittwirkung des Grundrechts auf Datenschutz

Als Besonderheit unter den österreichischen Grundrechten findet sich schließlich durch die Kompetenzbestimmung in § 1 Abs 5 DSG die Anordnung einer unmittelbaren Drittwirkung.[128] Daraus folgt, dass der Einzelne nicht nur vor Eingriffen durch den Staat, sondern auch gegen Eingriffe durch private Rechtsträger geschützt ist. Das Grundrecht auf Datenschutz ist verfassungsgesetzlich damit nicht nur (wie bei den klassischen Grundrechten) als subjektiv-öffentliches Recht, sondern auch als subjektives Privatrecht garantiert.[129]

Allfällige Verletzungen des Grundrechts können sohin auf dem Zivilrechtsweg (zB durch Unterlassungs- oder Schadenersatzklagen)[130] geltend gemacht werden. Einzig das Recht auf Auskunft ist auch im privaten Bereich vor der DSK geltend zu machen.[131]

2. Der Schutz personenbezogener Daten durch Art 8 EMRK

a) Personenbezogene Daten als Bestandteil der Privatsphäre iSd Art 8 EMRK

Das Recht auf Datenschutz ist va auch ein Bestandteil des Schutzes der Privatsphäre[132]; dieser wird in Österreich durch die im Verfassungsrang[133] stehende Bestimmung des

---

[127] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (2006) 13; *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 15 Rz 16; *Berka*, Geheimnisschutz Datenschutz Informationsschutz im Lichte der Verfassung in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 61.
[128] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 29.
[129] *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 74 Rz 92.
[130] Vgl §§ 32 und 33 DSG.
[131] § 1 Abs 5 1. Satz DSG.
[132] *Breitenmoser/Riemer/Seitz*, Praxis des Europarechts – Grundrechtsschutz (2006) 400.

Art 8 EMRK statuiert. Darin wird das Recht auf Schutz personenbezogener Daten zwar nicht ausdrücklich genannt, aus Abs 2 der Norm wird jedoch eine gewisse Nahebeziehung zum Datenschutz ersichtlich.

Im Vergleich zu § 1 DSG ist der Schutzbereich des Art 8 EMRK enger ausgestaltet, da nach der ersten Bestimmung auch andere Schutzgüter als das Privat- und Familienleben ein schutzwürdiges Interesse und somit ein Grundrecht auf Geheimhaltung begründen können.[134]

Zunächst werden in Art 8 Abs 1 EMRK vier verschiedene Rechte zusammengefasst: Das Recht auf Achtung des Privat- und Familienlebens, die Wohnung sowie die Korrespondenz. Datenschutzrechtlich relevant ist hierbei insb das Recht auf Achtung des Privatlebens, da die Privatsphäre des Einzelnen ihren Schutz hauptsächlich durch die Wahrung dieses Rechts erfährt.[135] Daraus resultiert, dass ein auf Art 8 EMRK fußendes Recht auf Datenschutz im Regelfall nur soweit reichen wird, wie der Schutzbereich des Rechts auf Privatleben.

Im Zuge der erforderlichen thematischen Einschränkung wird in Folge nur eine, datenschutzrechtlich besonders interessierende, Fragenstellung untersucht. Diese betrifft den Datenschutz als eigenständiges Element des Rechts auf Privatleben nach Art 8 EMRK.

IZm dieser Fragestellung hat va das Urteil *Rotaru*[136] des Europäischen Gerichtshofes für Menschenrechte (EGMR) Bedeutung. In diesem Urteil wurden Kriterien herausgearbeitet, durch die erstmals eine Beurteilung des Datenschutzes unter der EMRK unabhängig von der jeweils herrschenden Auffassung des begrifflichen Inhaltes des Privatlebens möglich wurde.[137]

---

[133] Bundesgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, BGBl 1964/59; *Öhlinger*, Verfassungsrecht[7] (2007) Rz 131.

[134] Vgl *Wiederin*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 95 Rz 136.

[135] *Siemen*, Datenschutz als europäisches Grundrecht (2006) 57.

[136] EGMR U 4.5.2000, *Rotaru*, Reports 2000-V, 28341/95.

[137] MwN *Siemen*, Datenschutz als europäisches Grundrecht (2006) 130.

Das Urteil *Rotaru* hat hierzu insb durch die Argumentation beigetragen, dass auch öffentliche Informationen (in diesem Fall politische und Publikationsaktivitäten) vom Schutzbereich des Art 8 Abs 1 EMRK erfasst sind, wenn diese nur ausreichend lange gespeichert werden.[138] Die zwingende Notwendigkeit einer Prüfung, ob diese Informationen trotz ihrer Öffentlichkeit das Privatleben betreffen kann der Entscheidung nicht entnommen werden.[139] Der EGMR kommt iE daher zu einer Loslösung des Datenschutzes vom Begriff des Privatlebens in Art 8 Abs 1 EMRK und manifestiert den Datenschutz sohin als eigenständiges Element des Rechts auf Privatleben.

b) Art 8 EMRK als Grundlage für ein Recht juristischer Personen auf Datenschutz?

In Bezug auf Unternehmen stellt sich im Folgenden die Frage, inwieweit diese als juristische Personen vom Schutz des Art 8 EMRK erfasst sein können. Ganz grds sind jedenfalls auch juristische Personen vom Regime der EMRK erfasst.[140] Unter den Schutztatbestand des „Privatlebens" im Sinne des Art 8 Abs 1 EMRK lassen sich deren personenbezogene Daten prima facie allerdings nur schwerlich subsumieren.

Der in Österreich offenkundig hA nach ist ein derartiges Privatleben zudem für juristische Personen gar nicht denkbar.[141] Des weiteren muss auf die Jud des VfGH hingewiesen werden, der dahingehend argumentierte, dass es nach Art 8 EMRK umstritten sei, ob Gesellschaften des Unternehmensrechts Träger des Grundrechts sein können – besonders dann, wenn die Unternehmensdaten zum Schutz von Rechten Dritter (zB Gläubiger und Aktionären) offengelegt werden müssen und keine die Privatsphäre von natürlichen Personen betreffenden Daten offengelegt werden müssen.[142]

---

138 http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=rotaru&sessionid =15299385&skin=hudoc-en (29.10.2008).

139 E veröffentlicht in ÖJZ 2001, 75.

140 Art 1 EMRK; *Frowein/Peukert*, Kommentar zur Europäische Menschenrechtskonvention[2] (1996) 19 Rz 3.

141 *Wiederin*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 31 Rz 38.

142 VfGH 12.12.2003, Slg 17.095; mwN ZfV 2004/1193.

Dem lässt sich mE jedoch entgegenhalten, dass sich der zivilrechtliche Begriff der Privatsphäre eng an den des Privatlebens in Art 8 Abs 1 EMRK anlehnt. Der Rsp des EGMR zufolge umfasst der Begriff des Privatlebens dabei sowohl geschäftliche als auch berufliche Aktivitäten.[143]

Hinzu kommt weiters, dass der EGMR in seiner Jud mittlerweile hinlänglich aus Art 8 EMRK ein Recht auf Datenschutz abgeleitet hat.[144]

IVm der eindeutigen Rsp des EGMR zur prinzipiellen Anwendbarkeit von Art 8 EMRK auf juristische Personen[145] folgt mE daraus, dass (zumindest auf europäischer Ebene) die Frage, ob ein Schutz personenbezogener Daten juristischer Personen bezüglich deren geschäftlicher und beruflicher Aktivitäten (und somit auch von Unternehmen einer entsprechenden Rechtsform) durch Art 8 EMRK besteht, zu bejahen ist.
Als primäre Grundlage zur Durchsetzung datenschutzrechtlicher Ansprüche wird sich Art 8 EMRK für Unternehmen in Österreich aufgrund der diesbezüglich negativen Rsp meiner Auffassung nach idR jedoch nicht als tauglich erweisen.

B. Ausgewählte Anwendungsfälle einfachgesetzlicher Grundlagen

1. Schadenersatzrechtliche Konsequenzen widerrechtlicher Datenverarbeitungen

Art 23 Abs 1 RL 95/46/EG verpflichtet die Mitgliedstaaten zum Erlass von Schadenersatzregelungen[146]; § 33 DSG stellt die Umsetzung dieser Richtlinienvorgabe im österr Recht dar.[147]

a) § 33 DSG als datenschutzrechtliche Spezialnorm

Zunächst gelten hierfür die allgemeinen Bestimmungen des Schadenersatzrechts, wonach eine Haftung nur bei Vorliegen von Verschulden in Betracht kommt. Für

---

[143] Vgl EGMR U 16.2.2000, *Amann*, RDJ 2000-II, 27798/95; ÖJZ 2001, 71.
[144] Vgl dazu EGMR U 25.2.1997, *Z.* gegen Finnland, RDJ 1997-IV, 323; EGMR U 27.8.1997, *M.S.* gegen Schweden, RDJ 1997-IV, 1437; EGMR U 28.1.2003, *Peck* , RDJ 2003-I, 123/163; *Meyer-Ladewig*, Europäische Menschenrechtskonvention, Handkommentar (2006) Art 8 Rz 11.
[145] EGMR 16.4.2002, *Societé Colas Est and others*, RDJ 2002-III, 37971/97; vgl dazu auch FN 122.
[146] *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) 262.
[147] ErläutRV 1613 BlgNR 20. GP 50.

besonders schwerwiegende Fälle rechtswidriger Datenverarbeitung sieht § 33 Abs 1 DSG auch den Ersatz immaterieller Schäden vor.

Ein derartiger Schadenersatzanspruch wird dann gewährt, wenn durch eine öffentlich zugängliche Verwendung von sensiblen Daten, strafrechtlich relevanten Daten oder Auskünften über die Bonität schutzwürdige Geheimhaltungsinteressen eines Betroffenen derart verletzt werden, dass dies im Ergebnis einer Bloßstellung im Sinne des MedienG gleichkommt.[148]

Bei einer öffentlichen Verwendung der genannten Daten kann der Betroffene daher einen Anspruch auf angemessene Entschädigung für die erlittene Kränkung gegen den Auftraggeber der Datenverarbeitung geltend machen. § 33 Abs 2 DSG statuiert außerdem eine (der Gehilfenhaftung des ABGB gleichende)[149] Haftung des Auftraggebers für schuldhaftes Verhalten seiner Leute soweit deren Tätigkeit für den Schaden ursächlich war.[150]

Aus der Formulierung des § 33 DSG folgt, dass ein immaterieller Schaden nur dann ersatzfähig ist, wenn eine der in Abs 1 der Bestimmung taxativ genannten Art von Daten betroffen ist.

Bei einer rechtswidrigen Verarbeitung jeder anderen Art von Daten ist der Verweis des § 33 Abs 1 erster S DSG auf die allgemeinen Bestimmungen des ABGB maßgeblich, wonach stets ein konkreter (Vermögens-) Schaden nachzuweisen sein wird. Gerade dieser Nachweis kann dem durch einen Verstoß gegen das DSG in seinen Rechten Verletzten in der Praxis jedoch erhebliche Schwierigkeiten bereiten.[151]

Unter Berücksichtigung dieses Umstandes ist va auf die Bestimmung des § 1328a ABGB, die den Schutz der Privatsphäre bezweckt, hinzuweisen. Im Unterschied zu § 33 DSG kann der Anspruch auf Schadenersatz hier zT nicht einmal

---

[148] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 242; vgl § 7 MedienG.
[149] Vgl § 1313a ABGB.
[150] MwN *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 33 Anm 5.
[151] *Knyrim*, Datenschutzrecht (2003) 249.

vom Vorliegen eines konkreten Vermögensschadens abhängig gemacht werden müssen.[152]

IE reicht daher eine erhebliche Verletzung der Privatsphäre als Klagegrund aus, womit bei Verletzungen des DSG (§ 33 DSG ist hierbei Schutzgesetz iSd § 1311 ABGB)[153] die Erhebung von Schadenersatzklagen generell erleichtert wird.

b) Bewertung der unternehmensbezogenen Relevanz

Vorerst ist festzuhalten, dass Unternehmen als juristische Personen bezüglich ihrer Geschäfts- und Betriebsgeheimnisse nicht durch die zuletzt dargestellte Bestimmung des § 1328a ABGB geschützt[154] sein können.

Dennoch wird neben der datenschutzrechtlichen Spezialnorm des § 33 DSG auch diese Bestimmung für Unternehmen als passiv Klagslegitimierte insofern von großer Bedeutung sein können, da sie sich bei einer unzulässigen Verarbeitung von zB Kunden- oder Mitarbeiterdaten leicht einer großen Zahl von Schadenersatzklagen gegenübersehen können.[155]

Zu denken ist etwa an die unzulässige Verarbeitung personenbezogener Daten in Schuldnerverzeichnissen, die nach einschlägiger Jud jedenfalls zu Schadenersatzansprüchen der Betroffenen führen kann. Hinzuweisen ist idZ etwa auf ein Urteil des OGH im Falle ein Rechtsanwaltes, der unter Verstoß gegen das Datenschutzgesetz in die „Warnliste der Banken" aufgenommen wurde. Die durch die widerrechtliche Eintragung verbreitete Annahme er sei als Rechtsanwalt kreditunwürdig, würde sein Ansehen bei Klienten und unter Kollegen untergraben und sei daher geeignet, seinen Ruf nachhaltig zu schädigen und sogar seine wirtschaftliche Existenz zu gefährden, so dass iE die Voraussetzungen für den Zuspruch eines immateriellen Schadens dem Grunde nach gegeben seien.[156]

---

[152] Dies freilich nur insoweit, als durch § 1328a ABGB der Ersatz des immateriellen Schadens gewährt wird.
[153] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 33 Anm 1.
[154] Vgl ErläutRV 173 BlgNR 22. GP 18.
[155] Dennoch wird auch in diesen Fällen ein grds Vorrang von § 33 DSG gegenüber § 1328a ABGB als lex specialis anzunehmen sein; idS auch *Koziol/Welser*, Bürgerliches Recht II[13] (2007) 348.
[156] OGH 15.12.2005, 6 Ob 275/05t.

Ein Schlussfolgerung die sich meiner Auffassung unschwer auch iZm anderen Berufsgruppen als zutreffend erweisen wird können und insofern die zunehmende Praxisrelevanz der Bestimmung des § 33 DSG belegt. Insbesondere auch die Benachrichtigung von Betroffenen im Vorfeld von Eintragungen in derartige Verzeichnisse wird vor dem Hintergrund des Grundsatzes der Datenverarbeitung nach Treu und Glauben[157] zu beachten sein.[158]

Aufgrund des expliziten Verweises in § 33 Abs 1 DSG wird im Anschluss der datenschutzrechtliche Gehalt der Bestimmung des § 7 MedienG untersucht.

[157] § 6 DSG.
[158] Vgl dazu *Koziol*, Der Grundsatz wonach Daten nur nach Treu und Glauben verarbeitet werden dürfen, erfordert eine Benachrichtigung des Betroffenen vor Eintragung in die Warnliste, ÖBA 2006, 530.

2. Der Schutz personenbezogener Daten durch das MedienG

Wird in einem Medium der höchstpersönliche Lebensbereich eines Menschen in einer Weise dargestellt, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen, hat der Betroffene gegen den Medieninhaber einen verschuldensunabhängigen Anspruch auf Entschädigung für die erlittene Kränkung.[159]

a) Zum datenschutzrechtlichen Gehalt der §§ 7, 7a und 7c MedienG

Geschützt wird sohin der höchstpersönliche Lebensbereich; Veröffentlichungen sind immer dann unzulässig, wenn sie ansehensmindernd sind, also geeignet sind, Interessen des Verletzten zu beeinträchtigen.[160] Der Begriff „Lebensbereich" umfasst dabei va das Leben mit der Familie, die Gesundheitssphäre und das Sexualleben.[161]

Aus der Formulierung „höchstpersönlich" resultiert eine Eingrenzung des Schutzgegenstandes insb auf den Bereich der Intimsphäre, so dass § 7 MedienG auf juristische Personen keine Anwendung findet.[162]

Jedenfalls nicht zum höchstpersönlichen Lebensbereich zählen die Vermögensverhältnisse, Unternehmensbeteiligungen sowie Angelegenheiten des Geschäfts- und Berufslebens.[163] Strafrechtlich relevante Daten sind vom Begriff dagegen mitumfasst.[164]

Ein Ersatzanspruch kann immer nur bei einer Bloßstellung gegeben sein; eine solche liegt vor, wenn das Ansehen des Betroffenen untergraben oder zumindest erschüttert oder auch wenn seine wirtschaftliche Existenz gefährdet worden ist.[165]

Bezüglich natürlicher Personen ist idZ auch auf § 7a MedienG hinzuweisen, der einen Schutz vor Bekanntgabe der Identität in besonderen Fällen (zB betreffend das Opfer

---

[159] § 7 Abs 1 MedienG.
[160] *Foregger/Litzka*, Mediengesetz[4] (2000) 55.
[161] *Foregger/Litzka*, Mediengesetz[4] (2000) 56.
[162] Vgl auch die Formulierung „ … höchstpersönliche Lebensbereich eines Menschen …" in § 7 Abs 1 MedienG, aus der sich eine Beschränkung auf natürliche Personen ableiten lässt.
[163] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 33 Anm 4.
[164] § 8 Abs 4 DSG.
[165] *Foregger/Litzka*, Mediengesetz[4] (2000) 56.

einer Straftat oder einen möglichen Tatverdächtigen) bezweckt, ohne dass ein überwiegendes öffentliches Interesse an den Angaben bestand. Weiters beachtlich ist § 7c MedienG, der dem Schutz vor verbotenen Veröffentlichungen dient und die Ermittlungsmethoden zur Bekämpfung der organisierten Kriminalität gewährleistet.[166]

b) Bewertung der unternehmensbezogenen Relevanz

Ob für juristische Personen bei widerrechtlichen Datenverarbeitungen überhaupt ein Schutz durch § 7 MedienG denkbar ist, ist fraglich. Dagegen spricht zu allererst die explizite Formulierung in Abs 1 der Bestimmung. Mit Inkrafttreten des VbVG[167] ist jedoch mittlerweile klargestellt, dass auch juristische Personen[168] Straftaten verantworten können, und somit als Betroffene strafrechtlich relevanter Daten, die wiederum vom Begriff des „Lebensbereichs" erfasst sind, in Betracht kommen können (in Frage käme etwa die Bloßstellung eines Unternehmens durch die Behauptung eines strafrechtlich relevanten Verhaltens wie zB geleisteten Schmiergeldzahlungen).

Das MedienG wird sich mE für Unternehmen als juristische Personen dennoch nicht zur Ahndung widerrechtlicher Datenverarbeitungen eignen, da im Zuge einer Wortinterpretation die begriffliche Festlegung des Gesetzgebers auf natürliche Personen und im Besonderen deren spezifische Schutzwürdigkeit iE deutlich überwiegt.[169]

3. Strafrechtliche Konsequenzen einer widerrechtlichen Datenverarbeitung nach dem DSG

a) §§ 51 und 52 DSG

§ 51 DSG stellt die absichtliche Schadenszufügung durch bestimmte Verwendungsformen von Daten und die rechtswidrige Übermittlung von Daten in Gewinnerzielungsabsicht unter Strafe. Die Bestimmung trägt der von der RL 95/46/EG

---

[166] Vgl *Karner*, Der zivilrechtliche Schutz von Geheimnissen, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 146.

[167] Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten (Verbandsverantwortlichkeitsgesetz – VbVG), BGBl I 2005/151 idF BGBl I 2007/112.

[168] § 1 Abs 2 VbVG.

[169] Vgl dazu auch die Ausführungen zu § 16 ABGB in Kap IV.B.5., wonach jedoch aus der Formulierung „Mensch" nicht zwingend eine Festlegung auf natürliche Personen folgen muss.

verlangten umfassenden Verpflichtung der Mitgliedstaaten zur Sicherstellung der vollen Anwendung der Bestimmungen der Richtlinie Rechnung.[170]

Strafbar macht sich, wer personenbezogene Daten benützt, Dritten zugänglich macht oder veröffentlicht, sofern ihm diese Daten aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder er sich diese widerrechtlich verschafft hat.[171] Personen, denen auf rein privatem Weg personenbezogene Daten anvertraut oder zugänglich gemacht worden sind, kommen als Täter daher nicht in Frage. Solche Personen können jedoch dann Täter sein, wenn sie sich die Daten ohne den Willen des Berechtigten und ohne anerkannten rechtlichen Grund verschafft haben; ob die Datenverschaffung hierbei auf beruflichem oder privatem Weg erfolgt ist, spielt keine Rolle.[172]

Hinsichtlich der subjektiven Tatseite wird Absicht bezüglich der Gewinnerzielung oder Schadenszufügung verlangt, wobei für die widerrechtliche Verschaffung der Daten bedingter Vorsatz ausreicht.[173] Der objektive Tatbestand ist erfüllt, wenn sich der Täter selbst einen Vermögensvorteil verschafft oder einem anderen einen Nachteil solcher Art zufügt, dass er Daten selbst benützt, einem anderen zugänglich macht oder veröffentlicht.[174]

Zusätzliche Voraussetzung einer Strafbarkeit ist, dass der Betroffene als Geheimnisträger ein schutzwürdiges Interesse an der Geheimhaltung seiner personenbezogenen Daten hat.[175] Ob ein derartiges Interesse besteht, ist anhand Art 8 EMRK iZm der Gesamtrechtsordnung zu beurteilen.[176] Schließlich ist darauf hinzuweisen, dass die Verfolgung des Delikts stets eine Ermächtigung durch den Verletzten erfordert.[177]

---

[170] Vgl ErwG 55 und Art 24 RL 95/46/EG; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 265.
[171] *Drobesch/Grosinger*, Das neue österreichische Datengesetz (2000) 286.
[172] *Hinterhofer*, Geheimnisschutz – Informationsschutz – Datenschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 183.
[173] *Dohr/Pollirer/Weiss*, DSG^2 I (2002) § 51 Anm 3.
[174] *Reindl*, Computerstrafrecht im Überblick (2004) 28.
[175] *Hinterhofer*, Geheimnisschutz – Informationsschutz – Datenschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 183.
[176] *Dohr/Pollirer/Weiss*, DSG^2 I (2002) § 51 Anm 6.
[177] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 51 Anm 1; vgl ErläutRV 1613 BlgNR 20. GP 53.

Ein Anwendungsfall der Bestimmung in der unternehmerischen Praxis könnte zB darin bestehen, dass ein ausscheidender Angestellter Kunden- und Lieferantendateien inklusive Telefonnummern und Ansprechpersonen auf einen eigenen Datenträger kopiert, um sie für sich zu nutzen oder Dritten zu verkaufen.[178]

Keine gerichtliche, sondern eine verwaltungsrechtliche Strafbestimmung stellt die Norm des § 52 DSG dar. Diese enthält einen Katalog einschlägiger Verwaltungsstrafbestimmungen; diese lassen sich wiederum in zwei Gruppen gliedern: § 52 Abs 1 DSG enthält solche Tatbestände, deren Merkmal eine tatsächliche Verletzung von Rechten ist, während § 52 Abs 2 DSG Tatbestände aufzählt in denen zwar noch keine Rechtsverletzung feststeht, aber Unterlassungen begangen wurden aus denen eine Gefährdung von Betroffenenrechten oder wenigstens eine Gefährdung der Durchsetzbarkeit dieser Rechte resultieren.[179]

Die Zurechnung der Verantwortlichkeit für Tathandlungen zu den einzelnen Mitarbeitern bzw Organen eines Auftraggebers oder Dienstleisters ist durch die Bestimmung des § 9 VStG[180] geregelt.[181]

Zu beachten ist die doppelte Subsidiaritätsklausel[182] wonach ein Verhalten nur dann nach dieser Bestimmung strafbar ist, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet und Verwaltungsstrafbestimmungen die für eine solche Handlung eine strengere Strafe vorsehen vorgehen.

Als Verwaltungsübertretung ist gem § 52 Abs 1 DSG das vorsätzliche Eindringen in eine Datenanwendung (Z 1), das vorsätzliche Übermittlung von Daten in Verletzung des Datengeheimnisses[183] (Z 2), das Verharren im rechtswidrigen Zustand (Z 3), der

---

[178] E 1 zu § 51 DSG in *Dohr/Pollirer/Weiss*, DSG[2] I (2002) 308; darauf Bezug nehmend *Knyrim*, Datenschutzrecht (2003) 242; vgl dazu auch *Jahnel*, Kein Schutz von Unternehmensdaten nach dem DSG? RdW 2005, 244.

[179] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 52 Anm 1; *Drobesch/Grosinger*, Das neue österreichische Datengesetz (2000) 289; ErläutRV 1613 BlgNR 20. GP 54.

[180] Verwaltungsstrafgesetz 1991 – VStG, BGBl 1991/52 idF BGBl I 2008/5.

[181] *Drobesch/Grosinger*, Das neue österreichische Datengesetz (2000) 290; *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 52 Anm 1.

[182] § 51 Abs 1 erster Teilsatz DSG.

[183] § 15 DSG.

Verstoß gegen das Löschungsverbot[184] (Z 4) sowie das arglistige Verschaffen von Daten über Katastrophenopfer[185] (Z 5) zu ahnden. Die Sanktion bei der Verwirklichung einer der Tatbestände besteht dabei in einer Geldstrafe von bis zu € 18.890,--.

Gem § 52 Abs 2 DSG ist eine Verletzung der Meldepflicht[186] (Z 1), die genehmigungslose Übermittlung von Daten ins Ausland[187] (Z 2), ein Verstoß gegen Offenlegungs- oder Informationspflichten[188] (Z 3) sowie die Außerachtlassung erforderlicher Sicherheitsmaßnahmen[189] (Z 4) mit einer Geldstrafe von bis zu € 9.445,-- bedroht.

Bei allen Delikten, die als Schuldform Vorsatz erfordern ist gem § 52 Abs 3 DSG bereits der Versuch strafbar. Auch der Verfall von Datenträgern oder Programmen (also der Software, nicht der Hardware) kann ausgesprochen werden, wenn diese mit der Verwaltungsstraftat in Zusammenhang stehen.

Als eine der wesentlichsten Änderungen gegenüber der alten Rechtslage nach dem DSG 1978 stellt sich der Umstand dar, dass die DSK im Verwaltungsstrafverfahren keine Zuständigkeit als Berufungsinstanz mehr besitzt. Dies verbietet sich, da der Grundsatz des fairen Verfahrens nicht gestattet, dass die DSK einerseits Kontrollrechte ausübt und im Rahmen dieser Kontrollbefugnisse gegebenenfalls auch Anzeige an die zuständige Strafbehörde erster Instanz erstattet und andererseits als Berufungsinstanz zur Entscheidung über diese Anzeige berufen wäre.[190]

Im Verwaltungsstrafverfahren ist nunmehr der unabhängige Verwaltungssenat als Berufungsinstanz jenes Bundeslandes zuständig, in dem die Behörde, die den Bescheid erlassen hat ihren Sitz hat.[191]

---

[184] § 26 Abs 7 DSG.
[185] § 48a DSG.
[186] § 17 DSG.
[187] § 13 DSG.
[188] §§ 24, 25 und 26 DSG.
[189] § 14 DSG.
[190] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 52 Anm 1.
[191] § 51 VStG iVm § 129a Abs 1 Z 1 B-VG; vgl *Dohr/Pollirer/Weiss*, DSG^2 I (2002) 315.

b) Bewertung der unternehmensbezogenen Relevanz

Va die Verwaltungsstrafbestimmung des § 52 DSG wird für Unternehmen der Privatwirtschaft mE eine nicht zu unterschätzende Relevanz haben: Während § 52 Abs 1 Z 1 DSG nur dann zur Anwendung gelangt, wenn das Unternehmen bewusst handelt, indem es sich widerrechtlich Zugang zu einer Datenanwendung verschafft, kann ein Verstoß gegen § 52 Abs 1 Z 2 DSG leicht ohne ein entsprechendes Bewusstsein erfolgen.

So dürfen zB Kundendaten, die für die Erfüllung eines bestimmten Auftrags gespeichert wurden, nicht ohne weiteres für Werbezwecke verwendet werden, da dies aufgrund der eigenmächtigen Änderung des Verwendungszwecks der Daten einen Verstoß gegen das Datengeheimnis bedeuten kann.[192] Auch gehen mit gesellschaftsrechtlichen Umstrukturierungen oftmals Übermittlungen personenbezogener Daten ins Ausland einher. Da diese zT genehmigungspflichtig sind, ist auch auf die in § 52 Abs 2 Z 2 DSG normierte Geldstrafe Bedacht zu nehmen, die im Falle einer Unterlassung der entsprechenden Genehmigungen verhängt werden kann.[193]

4. Der datenschutzrechtliche Gehalt der Delikte zum Geheimnisschutz nach dem StGB

Auch im Strafgesetzbuch finden sich Bestimmungen, die den Schutz gegen Verletzungen bestimmter (Berufs-) Geheimnisse zum Zweck haben.[194] Im Folgenden wird ein kurzer Überblick über jene Tatbestände gegeben, die im unternehmerischen Alltag von Bedeutung sein können.

a) §§ 118-124 u 148a StGB

§ 118 StGB dient dem Schutz der Vertraulichkeit des geschriebenen Wortes soweit dieses durch einen entsprechenden Verschluss gegen die Kenntnisnahme durch

[192] *Knyrim*, Datenschutzrecht (2003) 242; *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 52 Anm 5.
[193] Vgl dazu auch Kap V.F.
[194] Insofern kann aus Gründen der notwendigen thematischen Beschränkung der Untersuchung (mit Ausnahme der Bestimmung des § 148a StGB) in diesem Kap auch keine Behandlung des materiellen Computerstrafrechts geboten werden.

Unbefugte geschützt ist. Irrelevant ist dabei, ob der Inhalt des Schriftstückes Geheimnischarakter hat oder nicht. [195]

Abs 1 der Bestimmung pönalisiert das Öffnen verschlossener Briefe und Schriftstücke, Abs 2 stellt bestimmte gleichgestellte Begehungsweisen unter Strafe (wie etwa das Öffnen eines Schreibtisches oder Aktenschrankes)[196] sowie den Einsatz von Umgehungstechniken zur Kenntniserlangung des Inhaltes. Schließlich macht sich nach Abs 3 strafbar, wer Briefe oder Schriftstücke vor der Kenntnisnahme durch den berechtigten Empfänger unterschlägt oder unterdrückt.

Da § 118 StGB als primären Schutzbereich bereits die „bloße Vertraulichkeit“ von verschlossenen Schriftstücken hat, wird die Norm mE mangels Spezialität in Hinblick auf den unternehmensspezifischen Bereich (so zB bei der Verletzung von Betriebsgeheimnissen) im Ergebnis jedoch keine vorrangige Bedeutung erreichen können.

§ 118a StGB dient dem Schutz der Vertraulichkeit von gespeicherten Daten.[197] Eine Tathandlung nach dieser Bestimmung setzt dabei, wer sich Zugang zu einem Computersystem (oder zu einem Teil) verschafft und dabei eine spezifische Sicherheitsvorkehrung im System überwindet.[198] Unter dem Begriff „Computersystem“ sind dabei sowohl Netzwerke als auch einzelne PCs oder Notebooks zu verstehen.[199]

§ 118a StGB richtet sich in erster Linie gegen sog „Hacker“. Ein tatbestandsmäßiges Verhalten kann dabei bspw iZm Vorbereitungshandlungen zur Industriespionage gegeben sein; etwaige Konkurrenzen sind auch zu den §§ 119 und 126a StGB denkbar.[200]

§ 119 StGB schützt die Vertraulichkeit von (Tele-) Kommunikation und computersystemgestützter Nachrichtenübermittlung gegenüber Abhörvorrichtungen (iE

---

[195] *Lewisch* in WK^2 (2008) § 118 Rz 1.
[196] *Lewisch* in WK^2 (2008) § 118 Rz 20.
[197] Vgl dazu *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 181.
[198] *Reindl-Krauskopf* in WK^2 (2008) § 118a Rz 19.
[199] Vgl § 74 Abs 1 Z 8 StGB.
[200] *Reindl-Krauskopf* in WK^2 (2008) § 118a Rz 41.

somit auch das nach Art 10a StGG[201] grundrechtlich geschützte Fernmeldegeheimnis).[202]

Als Abhörvorrichtung kommt dabei ein Gerät in Betracht, aber auch eine schädliche Software (wie zB ein „Trojaner“), die zum Zweck des Ausspionierens des E-Mail-Verkehrs eingeschleust wurde.[203] Nach dieser Bestimmung nicht geschützt sind jedoch gespeicherte oder noch nicht abgeschickte E-Mails (Entwürfe); dies, da nach hL nur der Übertragungsweg geschützt ist.[204]

§ 119a StGB ergänzt den nach § 119 StGB bestehenden Schutz des Kommunikationsgeheimnisses und soll das widerrechtliche Abfangen von Daten verhindern.[205] § 119a 1. Fall StGB pönalisiert die Benützung einer Vorrichtung, die an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde.[206] § 119a 2. Fall StGB bedroht denjenigen mit Strafe, der die elektronische Abstrahlung eines Computersystems abfängt.[207]

Die Praktische Relevanz dieses Delikts im Zuge des Auskundschaftens von Betriebsgeheimnissen wird meiner Auffassung nach auch hier aufgrund speziellerer Normen verhältnismäßig klein sein. Seitdem bei Due Diligence Prüfungen jedoch Datenräume[208] zunehmend rein elektronisch eingerichtet werden, sind gewisse Anwendungsfälle mE zumindest denkbar.[209]

§ 120 StGB dient dem Schutz des gesprochenen Wortes[210] außerhalb des Bereichs der Telekommunikation und schützt die Vertraulichkeit von nicht öffentlichen Äußerungen

---

[201] Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, RGBl 1867/142 idF BGBl 1988/684.
[202] *Lewisch* in WK^2 (2008) § 119 Rz 1.
[203] Vgl zu den möglichen Tathandlungen auch *Dohr/Pollirer/Weiss*, DSG^2 (2002) Anh V/1/C, 56.
[204] *Lewisch* in WK^2 (2008) § 119 Rz 9a.
[205] *Fabrizy*, StGB^9 (2006) § 119a Rz 1.
[206] *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 182.
[207] *Reindl-Krauskopf* in WK^2 (2008) § 119a Rz 10.
[208] S dazu Kap V.E.5.
[209] Vgl *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen, MR 2007, 341.
[210] MwN *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 120 Rz 30.

und Nachrichten.[211] Va wird der Missbrauch (die bloße Aufnahme eines Gespräches ist noch nicht strafbar)[212] von Tonband- oder Abhörgeräten und die Weitergabe von im Zuge dessen rechtswidrig erlangten Tonaufnahmen pönalisiert.[213] Auch diese Bestimmung wird sich im wirtschaftsrechtlichen Kontext, insb in Folge der grds Beschränkung des Schutzbereiches auf das gesprochene Wort (Anwendungsfälle können sich jedoch im Bereich der Datenspionage ergeben)[214] nur sehr eingeschränkt zur Wahrung betrieblicher Geheimnisse eignen.

Die nun folgende Gruppe von Delikten hat dagegen eine verhältnismäßig große Bedeutung für den Schutz von personenbezogenen Daten und sonstigen Informationen im unternehmerischen Alltag.

Vorerst ist festzuhalten, dass das österreichische Strafrecht keinen umfassenden Schutz von Berufsgeheimnissen gewährt. Ein gesetzlicher Schutz besteht dabei nur für jene Teilbereiche, die dem Gesetzgeber als so gefährdet gegenüber entsprechenden Beeinträchtigungen erschienen, dass er hierfür einen gesetzlichen Schutz implementierte.[215]

§ 121 StGB pönalisiert die Offenbarung oder Verwertung gesundheitsbezogener Geheimnisse durch Angehörige gesetzlich geregelter Gesundheitsberufe oder bestimmter medizinisch-administrativer Berufsgruppen; weiters die Geheimnisverwertung durch gerichtlich oder verwaltungsbehördlich bestellte Sachverständige.[216]

Im unternehmerischen Alltag sind tatbestandsmäßige Handlungen mE nicht sehr wahrscheinlich; aus datenschutzrechtlicher Perspektive ist darauf hinzuweisen, dass gesundheitsbezogene Geheimnisse jedenfalls sensible Daten im Sinne des § 4 Z 2 DSG

---

[211] *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 173.
[212] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 120 StGB Anm 2.
[213] *Lewisch* in WK[2] (2008) § 120 Rz 1.
[214] § 120 Abs 2a StGB; *Lewisch* in WK[2] (2008) § 120 Rz 31d; vgl dazu auch *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 120 Rz 67.
[215] *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 174.
[216] *Lewisch* in WK[2] (2008) § 121 Rz 1.

sind und nur unter den strengen Voraussetzungen des § 9 DSG verarbeitet werden dürfen.[217]

§ 122 StGB gewährt einen Schutz gegen die Offenbarung und Verwertung von Geschäfts- oder Betriebsgeheimnissen durch Personen, die als Organwalter bei behördlichen Untersuchungen und Überprüfungen Kenntnis von Wirtschaftsgeheimnissen erlangen.[218] Die Bestimmung dient in erster Linie der kriminalstrafrechtlichen Absicherung von bestehenden gesetzlichen Geheimhaltungspflichten.[219]

Während ein Teil der Lehre[220] daraus schließt, dass zB Kaufinteressenten die (etwa im Rahmen einer Due Diligence Prüfung erfahrenen) Geschäftsgeheimnisse rechtswidrig offenbaren oder verwerten nicht unter § 122 StGB subsumiert werden können, stellt eine andere Meinung[221] nur auf das Kriterium einer Kenntniserlangung im Rahmen beruflicher Tätigkeit ab und kommt damit iE zu einer Strafbarkeit auch ohne gesetzliche oder behördliche Anordnung der Kontrolltätigkeit.

Besonders im Vorfeld von Unternehmenskäufen kann § 122 StGB mE nicht unerhebliche Bedeutung zukommen (hinzuweisen ist idZ va auf die gesellschaftsrechtlichen Verschwiegenheitspflichten von Geschäftsführen oder Vorstandsmitgliedern).[222]

Eine definitiv wirtschaftsrechtliche Zielsetzung hat die Bestimmung des § 123 StGB. Sie pönalisiert die ungerechtfertigte Verschiebung von Informationen durch Industriespionage.[223]

Strafbar ist das Auskundschaften von Geschäfts- und Betriebsgeheimnissen, wobei unter „Auskundschaften“ jede Tätigkeit zur Erlangung eines Wirtschaftsgeheimnisses zu verstehen ist.[224] Da sich dieser Begriff entsprechend weit darstellt und somit zu einer nicht intendierten Kriminalisierung führen kann, ist jedoch eine einschränkende

---

[217] Vgl dazu § 9 Z 11 DSG der für Unternehmen bspw im Rahmen einer betrieblichen Gesundheitsvorsorge Bedeutung haben kann; mwN *Knyrim*, Datenschutzrecht (2003) 110.
[218] *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 122 Rz 6.
[219] *Lewisch* in WK^2 (2008) § 122 Rz 13.
[220] *Lewisch* in WK^2 (2008) § 122 Rz 6.
[221] *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 122 Rz 45; *Ruhm*, Haftung des Aufsichtsrates einer AG bei pflichtwidriger Weitergabe von Geschäftsinformationen, RdW 2005, 813.
[222] Vgl dazu auch *Dohr/Pollirer/Weiss*, DSG^2 I (2002) § 122 StGB Anm 4.
[223] *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 123 Rz 1.
[224] MwN *Lewisch* in WK^2 (2008) § 123 Rz 4.

Interpretation angebracht.[225] § 123 StGB ist zweifellos eine der Kernstrafnormen des unternehmerischen Geheimnisschutzes und als solche von eminenter Bedeutung.[226]

§ 124 StGB pönalisiert den sog „wirtschaftlichen Landesverrat“ (Industriespionage zugunsten des Auslands).[227] Unter Strafe steht die Auskundschaftung bzw Preisgabe von inländischen Wirtschaftsgeheimnissen zu Gunsten des Auslands. Vor dem Hintergrund des europäischen Binnenmarktes ist diese Bestimmung jedoch der hL nach überholt und wird sich unter Zugrundelegung eines modernen marktwirtschaftlichen Verständnisses daher nur sehr bedingt zum Schutz von Wirtschaftsgeheimnissen eignen.[228]

Von nicht unerheblicher Bedeutung ist dagegen die Bestimmung des § 148a StGB; als Vermögensdelikt ausgestaltet stellt es den betrügerischen Verarbeitungsmißbrauch von Daten unter Strafe. Wesentliches Merkmal des Delikts ist der missbräuchliche Umgang mit Daten, der über die Schädigung eines anderen zu einer unrechtmäßigen Bereicherung des Täters oder eines Dritten führen soll.[229] Hinzuweisen ist darauf, dass die Bestimmung in echter Konkurrenz zu § 51 DSG stehen kann.[230] Als Qualifikation enthält § 148a StGB die gewerbsmäßige Begehung der Tat; bei Vorliegen dieses Schuldmerkmals kann eine bis zu zehnjährige Freiheitsstrafe ausgesprochen werden.

b) Bewertung der unternehmensbezogenen Relevanz

Die Bestimmungen der §§ 118 – 120 StGB sind aufgrund der oa Zielsetzungen für den unternehmerischen Bereich von eher untergeordnete Bedeutung. Die §§ 121 u 122 StGB pönalisieren dagegen explizit den Verrat von Berufsgeheimnissen und sind

---

[225] *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 123 Rz 24.
[226] Beachtlich ist jedoch, dass das Auskundschaften von Wirtschaftsgeheimnissen nach § 123 StGB mit höherer Strafe als deren Verwertung nach § 122 StGB bedroht ist; vgl *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 178, der diese gesetzgeberische Wertung für fragwürdig erachtet.
[227] *Lewisch* in WK^2 (2008) § 124 Rz 1; *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 124 Rz 5.
[228] *Lewisch* in WK^2 (2008) § 124 Rz 3 und 4; *Thiele* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB II (2007) § 124 Rz 4; vgl dazu auch *Hinterhofer*, Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 178.
[229] *Triffterer* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Sbg Kommentar zum StGB III (1992) § 148a Rz 3.
[230] *Kirchbauer/Presslauer* in WK^2 (2006) § 146 Rz 184.

insofern von größerer Relevanz. Dennoch wird auch hier durch die verhältnismäßig enge Beschreibung des Täterkreises die tatsächliche Bedeutung im wirtschaftlichen Alltag mE verhältnismäßig gering sein.

Die Bestimmungen des § 123 StGB stellt sich dagegen als Kernstrafnorm des Geheimnisschutzes dar und ist insofern von immanenter Bedeutung. Im Falle des § 124 StGB werden mE jedoch, insb in Anbetracht des europäischen Binnenmarktes, wenig Anwendungsfälle denkbar sein.

Für den unternehmerischen Bereich jedenfalls von Bedeutung ist dagegen die Bestimmung des § 148a StGB: So kann ein Eingriff in eine Datenverarbeitung, die mit „Gewinnabsicht" durchgeführt wird (zu denken ist bspw an einen Verkauf von Informationen aus einer Datenbank durch einen Mitarbeiter zum Nachteil eines Unternehmens), neben entsprechenden zivilrechtlichen auch zu massiven strafrechtlichen Konsequenzen wie einer langjährigen Freiheitsstrafe führen.[231]

Als wesentlicher Unterschied zum DSG sind von den Bestimmungen des StGB zum Geheimnisschutz va auch nicht personenbezogene Daten erfasst. In jenen Bereichen, die Überschneidungen aufweisen, wird sich mE ein Geheimhaltungsschutz nach dem Strafgesetzbuch auf Grund der deutlich schärferen Sanktionen im Einzelfall sogar als effektiver erweisen können.[232]

Zusammenfassend stehen daher jedenfalls auch nach dem StGB Mittel zum Schutz von Daten zur Verfügung. Für Entscheidungsträger wie Geschäftsführer oder Vorstände umzustrukturierender Unternehmen ist dabei insb die Möglichkeit einer strafrechtlichen Verantwortlichkeit nach dem VbVG zu beachten.[233]

Aufgrund des Zielsetzung dieser Arbeit kann an dieser Stelle keine eingehende Untersuchung der grds dogmatischen Erwägungen zur noch sehr jungen Rechtsmaterie

[231] *Knyrim*, Datenschutzrecht (2003) 241.
[232] Zu den generalpräventiv wohl wenig wirksamen Strafobergrenzen im DSG vgl auch grds *Kotschy*, Verwaltungsbehördlicher Rechtsschutz in Datenschutzangelegenheiten, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 132.
[233] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 1 VbVG Anm 2 und § 2 VbVG Anm 1.

des VbVG geboten werden.[234] Im Anschluss sollen dennoch die im unternehmerischen Zusammenhang interessierenden Grundfragen kurz dargestellt werden.

c) Strafbarkeit des Unternehmens selbst als juristische Person durch Verletzung des Datenschutzes?

Als maßgebliche Bestimmung stellt sich § 3 VbVG dar. Hierin ist geregelt, unter welchen Voraussetzungen ein Verband[235] (idZ eine Gesellschaft als Rechtsträgerin des Unternehmens) für Straftaten seiner Entscheidungsträger oder Mitarbeiter verantwortlich ist.

Im Fall des § 3 Abs 2 VbVG kann der Verband als unmittelbar für die Handlung des Entscheidungsträgers verantwortlich gemacht werden. Entscheidungsträger sind hierbei typischerweise Geschäftsführungsorgane des Unternehmens.[236] Für das Handeln von Mitarbeitern kann das Unternehmen haftbar gemacht werden, wenn diese die Tat rechtswidrig und vorsätzlich oder unter Außerachtlassung der gebotenen Sorgfalt begangen haben und die Begehung ermöglicht oder dadurch erleichtert wurde, dass die Entscheidungsträger die gebotenen technischen, organisatorischen oder personellen Maßnahmen zur Verhinderung solcher Taten unterlassen haben.[237]

Da eine Strafbarkeit von natürlichen und juristischen Personen auch nebeneinander möglich ist, kann bspw im Fall von Industriespionage durch einen Mitarbeiter sowohl eine Haftung dessen selbst nach dem StGB[238] als auch seines Unternehmens nach dem VbVG in Betracht kommen.[239]

Eine definitive Beurteilung der unternehmensbezogenen Relevanz des VbVG iZm Verstößen gegen den Datenschutz kann zum gegenwärtigen Zeitpunkt jedoch nicht gegeben werden. Wie letzteres Bsp allerdings zeigt scheinen konkrete Anwendungsfälle zumindest denkbar; in der aktuellen höchstgerichtlichen Jud finden sich bis dato

---

[234] Dazu weiterführend *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG (2007) 53 ff.
[235] Zum begrifflichen Inhalt des Verbandes s *Rauter*; Verband, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 323.
[236] So etwa der Vorstand einer AG.
[237] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 3 VbVG Anm 2.
[238] Diesfalls nach § 123 StGB.
[239] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 3 VbVG Anm 3.

jedenfalls noch keine Verurteilungen nach dem VbVG.[240] Inwieweit diesem im oa Zusammenhang Bedeutung zukommt wird sich daher erst in Zukunft erweisen können.

5. Datenschutz als Persönlichkeitsrecht

a) Datenschutzrechtliche Interpretation des § 16 ABGB

§ 16 ABGB stellt in der österreichischen Rechtsordnung eine der zentralen Grundlagen für die Anerkennung einer Anzahl von subjektiven Rechten dar, die sowohl juristischen als auch natürlichen Personen zustehen.[241]

Im datenschutzrechtlichen Kontext interessiert va das Recht auf Wahrung der Geheimsphäre. Grds von der hL bereits anerkannt[242], wurde es durch den OGH in einer grundlegenden Entscheidung[243] im Jahr 1978 erstmals eindeutig als Persönlichkeitsrecht präzisiert. Dieses schützt sowohl gegen das Eindringen in die Privatsphäre der Person als auch gegen die Verbreitung rechtmäßig erlangter Informationen aus der und über die Geheimsphäre; dies gilt auch für das Berufs- und Geschäftsleben, ohne dass Berufs- und Geschäftsgeheimnisse über § 16 ABGB geschützt sind. [244]

Das durch § 1 DSG eingeräumte Recht auf Auskunft, Richtigstellung und gegebenenfalls Löschung von Daten ist zweifellos als Persönlichkeitsrecht iSd § 16 ABGB zu sehen.[245] Im Zuge der hier interessierenden wirtschaftlichen Betrachtungsweise stellt sich nun die Frage, ob Unternehmen (insb als juristische Personen) bezüglich ihrer Daten des Geschäftslebens einen Schutz aus der Bestimmung des § 16 ABGB ableiten können.

Eine grundlegende Erörterung dieser Frage vermag jedoch an dieser Stelle nicht gegeben zu werden, da insb die Notwendigkeit der inhaltlichen Abgrenzung des Begriffs der Geheimsphäre bei juristischen Personen sowie die im Zuge dessen zu behandelnden Fragestellungen höchst komplex sind und im Rahmen dieser Arbeit nicht

---

[240] S dazu das Rechtsinformationssystem des Bundeskanzleramts http://www.ris.bka.gv.at/Jus/ (13.9.2009).
[241] *Posch* in *Schwimann*, ABGB[3] I (2005) § 16 Rz 3; vgl dazu auch § 26 2. Satz ABGB.
[242] Vgl *Klang*, ABGB I (1964) § 16 Anm 2.
[243] OGH 24.10.1978, 4 Ob 91/78.
[244] *Aicher* in *Rummel*, ABGB[3] I (2000) § 16 Rz 24.
[245] *Posch* in *Schwimann*, ABGB[3] I (2005) § 16 Rz 42; *Aicher* in *Rummel*, ABGB[3] I (2000) § 16 Rz 24a.

erschöpfend behandelt werden können.[246] Hingewiesen werden muss an dieser Stelle auch auf § 1328a ABGB, der den Schutz der Privatsphäre bezweckt; diesbezüglich darf auf die Ausführungen in Kap IV.B.1. verwiesen werden.

Außer Zweifel steht jedenfalls, dass sowohl natürliche als auch juristische Personen aus der Bestimmung des § 16 ABGB als Persönlichkeitsrecht ein Recht auf Schutz ihrer personenbezogenen Daten ableiten können. [247]

b) Bewertung der unternehmensbezogenen Relevanz

Meiner Ansicht nach wird die allgemeine Norm des § 16 ABGB für die Rechtsdurchsetzung entsprechender Ansprüche im Einzelfall in ihrer Bedeutung deutlich hinter das Grundrecht auf Datenschutz nach § 1 DSG zurücktreten, insb aufgrund der diesbezüglich wesentlich detaillierteren Ausgestaltung.[248]

Ein Anwendungsfeld der Bestimmung bietet sich jedenfalls im arbeitsrechtlichen Kontext, hierbei werden im Gros der Fälle jedoch ausschließlich natürliche Personen erfasst sein.[249]

6. Die Geheimhaltung von (personenbezogenen) Daten im Gesellschaftsrecht

Gerade im Gesellschaftsrecht können sich durch die Regelungen zum Geheimnisschutz im Hinblick auf den Schutz personenbezogener Daten interessierende Überschneidungen mit dem Regime des DSG ergeben. Im Anschluss werden daher jene Bestimmungen des GmbHG und AktG untersucht, bei denen derartige Implikationen am wahrscheinlichsten sind.

---

[246] Statt vieler *Fellner*, Persönlichkeitsschutz juristischer Personen (2007) 182.
[247] IdS auch ErläutRV 1613 BlgNR 20. GP 50.
[248] Vgl idZ die in § 1 Abs 3 Z 1 u 2 DSG normierten Betroffenenrechte.
[249] S dazu Kap VIII.

a) § 24 GmbHG und §§ 84 und 99 AktG

Zuerst weist als eine im Gesellschaftsrecht zentrale Norm va die Bestimmung des § 24 GmbHG Berührungspunkte mit dem Datenschutz auf.

Grundlegender Regelungsinhalt der Bestimmung ist die Hintanhaltung eines möglichen Konfliktes zwischen den eigenen Interessen der Geschäftsführer einer Gesellschaft und ihren Pflichten gegenüber selbiger.[250] Dem Gesetzeswortlaut nach normiert § 24 GmbHG in erster Linie ein Wettbewerbsverbot; diesem zufolge dürfen die Geschäftsführer ohne Einwilligung der Gesellschaft weder Geschäfte in deren Geschäftszweig für eigene oder fremde Rechnung machen, noch sich bei einer Gesellschaft des gleichen Geschäftszweiges als persönlich haftende Gesellschafter beteiligen oder eine Stelle im Vorstand oder Aufsichtsrat oder als Geschäftsführer bekleiden.[251]

Aus dieser generellen Anordnung der Vermeidung eines potentiell gesellschaftsschädigenden Verhaltens erfließt jedoch auch eine, im Gesetz nicht ausdrücklich ausgesprochene, Verpflichtung der Geschäftsführer zur Geheimhaltung von Geschäfts- und Betriebsgeheimnissen (zum Inhalt dieser Begriffe gleich mehr).[252]

Weiters besteht eine Verpflichtung zur Verschwiegenheit über Tatsachen und Betriebsinterna, an deren Geheimhaltung die GmbH ein schutzwürdiges Interesse hat.[253] Dabei müssen die Geschäftsführer die Gesellschaft jedenfalls vor Nachteilen aus der Verletzung solcher Geheimnisse schützen, die mit der Sorgfalt eines ordentlichen Geschäftsmannes zu bewahren sind.[254]

Diese Verschwiegenheits- und Geheimhaltungspflichten können dabei auch insb nach Beendigung der Geschäftsführertätigkeit andauern, sofern sie das eigene Weiterkommen des Geschäftsführers nicht unverhältnismäßig beeinträchtigen.[255] Als

---

[250] *Koppensteiner/Rüffler* , GmbHG-Kommentar[3] (2007) § 24 Rz 1.
[251] § 24 Abs 1 GmbHG; vgl dazu auch § 112 Abs 1 UGB.
[252] *Mader*, Kapitalgesellschaften[6] (2008) 23: *Koppensteiner/Rüffler* , GmbHG-Kommentar[3] (2007) § 24 Rz 18; vgl dazu auch *Duursma/Duursma-Kepplinger/Roth*, Handbuch zum Gesellschaftsrecht (2007) Rz 2957.
[253] *Reich-Rohrwig*, Das österreichische GmbH-Recht[2] (1997) § 24 Rz 2/302.
[254] *Gellis/Feil*, Kommentar zum GmbHG[6] (2006) § 24 Rz 7; vgl § 25 Abs 1 GmbHG.
[255] *Reich-Rohrwig*, Das österreichische GmbH-Recht[2] (1997) § 24 Rz 2/303.

Rechtsfolgen eines Verstoßes gegen § 24 GmbHG kommen ua die Möglichkeit zur sofortigen Abberufung des Geschäftsführers sowie ein Anspruch der Gesellschaft auf Schadenersatz (Verschulden vorausgesetzt) in Betracht.[256] Den Geheimhaltungspflichten nach dem GmbHG kann besonders bei gesellschaftsrechtlichen Umstrukturierungen große Bedeutung zukommen, da es gerade bei den Mitgliedern der beteiligte Leitungsorgane zu Interessenskonflikten kommen kann; ist bspw ein Aufsichtsrat vorhanden, können diesem uU auch Vertreter konkurrierender Unternehmen angehören.

Auch das AktG kennt die Geheimhaltung bestimmter Informationen als wesentliches Element der gesellschaftsrechtlichen Treue- und Sorgfaltspflicht.[257] Nach den Bestimmungen der §§ 84 Abs 1 S 2 und § 99 AktG, sind Vorstands- und Aufsichtsratmitglieder dazu angehalten, über vertrauliche Angaben Stillschweigen zu bewahren.

Im Grunde wird damit die sich bereits aus der Organstellung ergebende Verpflichtung von Vorstands- und Aufsichtratsmitgliedern, keine vertraulichen Informationen nach außen hin weiterzugeben wiederholt.[258] Die Pflicht zur Verschwiegenheit endet, wenn die Tatsache öffentlich bekannt wurde oder vom Vorstand bekannt gemacht oder klargestellt wurde, dass ein Geheimhaltungsinteresse nicht mehr gegeben ist.

Von der Verschwiegenheitspflicht umfasst sind Betriebs- und Geschäftsgeheimnisse.[259] Unter dem Begriff des Geheimnisses sind dabei Tatsachen und Erkenntnisse zu verstehen, die entweder nur dem betreffenden Vorstandsmitglied oder nur dem Vorstand als Kollegialorgan oder nur dem Vorstand und dem Aufsichtsrat oder auch nur einem kleinen überschaubaren, zur Geheimhaltung verpflichteten Kreis von Personen bekannt sind und die anderen Personen nicht oder nur sehr schwer zugänglich sind.[260]

Diese Tatsachen und Erkenntnisse werden dann zu einem Betriebs- oder Geschäftsgeheimnis, wenn sie sich auf Betriebe des Unternehmens oder auf das

---

[256] *Koppensteiner/Rüffler* , GmbHG-Kommentar[3] (2007) § 24 Rz 14; vgl § 24 Abs 3 GmbHG.
[257] *Jabornegg/Strasser*, Kommentar zum AktG[4] (2001) § 84 Rz 86.
[258] *Doralt/Nowotny/Kalss*, Aktiengesetz (2003) § 84 Rz 12; vgl *Kalss*, Geheimnisschutz – Datenschutz – Informationsschutz im Gesellschaftsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 245.
[259] *Mader*, Kapitalgesellschaften[6] (2008) 72.
[260] MwN *Jabornegg/Strasser*, Kommentar zum AktG[4] (2001) § 84 Rz 87.

Unternehmen selbst beziehen und seitens des Gesellschaft klar ist, dass die Weitergabe der entsprechenden Informationen für sie nachteilig sein kann.[261]

Unter „vertraulichen Angaben“ werden daher va solche Informationen zu verstehen sein, deren Geheimhaltung im objektiven Gesellschaftsinteresse liegt; im unternehmerischen Bereich kann ein derartiges Geheimhaltungsinteresse zB an Einkaufskonditionen, Produktionsverfahren, patentierten Systemen oder detaillierten Kundenlisten bestehen. Auch vertrauliche Beratungen im Personalbereich, über schwebende Vertragsverhandlungen oder über den Forschungsstand im Technologiebereich werden sich dabei unter den Begriff der „vertraulichen Angaben“ subsumieren lassen.[262]

Jedoch können nicht nur objektive (personenbezogene) Daten, sondern auch subjektive Ansichten und Meinungen in diese Kategorie fallen, wie etwa die von einem Aufsichtsrats- oder Vorstandsmitglied bezüglich der Lage des Unternehmens oder eines bestimmten Geschäftsvorfalls getätigten Äußerungen.[263]

Als bereichsspezifische Regelung haben Vorstandsmitglieder von Kreditinstituten gem § 38 Abs 1 BWG (so wie auch alle Beschäftigten von Banken im Sinne des BWG) das Bankgeheimnis zeitlich unbegrenzt und somit de facto bis an ihr Lebensende ohne Rücksicht auf ihr Ausscheiden aus dem Rechtsverhältnis zur Bank zu wahren.[264]

§ 99 AktG stellt eine reine Verweisungsnorm dar; verwiesen wird auf die für Vorstandsmitglieder geltende Haftungsvorschrift des § 84 AktG; iE erfolgt die zentrale Regelung der Haftung (und damit auch der Verschwiegenheitspflicht) der Aufsichtsratmitglieder gegenüber der Gesellschaft für Pflichtverletzungen somit in identer Weise wie für Vorstandsmitglieder.[265]

---

[261] Vgl *Hofman*, Due Diligence – Grenzen und Möglichkeiten des Managements (2006) 146.
[262] *Feltl/Mosing*, Das Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 234.
[263] *Kalss*, Geheimnisschutz – Datenschutz – Informationsschutz im Gesellschaftsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 241.
[264] *Jabornegg/Strasser*, Kommentar zum AktG[4] (2001) § 84 Rz 90; mwN *Kalss*, Münchener Kommentar zum Aktiengesetz[3] (2008) § 93 dAktG Rz 313; vgl dazu Kap IV.B.11.
[265] *Jabornegg/Strasser*, Kommentar zum AktG[4] (2001) § 99 Rz 32.

Der Vollständigkeit halber sei an dieser Stelle auch auf gesellschaftsrechtliche Publizitätspflichten des Unternehmens hingewiesen. Diese erfordern regelmäßig eine Offenlegung unternehmensbezogener Daten; Bsp hierfür sind etwa die Offenlegung des Jahresabschlusses[266] sowie des Konzernabschlusses[267]. Da die Datenverwendung in diesen Fällen jedoch durch eine ausdrückliche gesetzliche Ermächtigung gerechtfertigt ist, besteht im gegenständlichen Zusammenhang kein Bedarf einer weiteren Problematisierung.

b) Bewertung der unternehmensbezogenen Relevanz

Zusammenfassend wird meiner Auffassung nach den aktienrechtlichen Regelungen zum Schutz von Geheimnissen (ebenso wie den GmbH-spezifischen Vorschriften) bei gesellschaftsrechtlichen Umstrukturierungen gerade iVm den diesbezüglichen datenschutzrechtlichen Bestimmungen große Bedeutung zukommen.

Wirtschaftliche Informationen wie Daten über Umsatz, Gewinn oder Verlust werden sich nämlich im Hinblick auf den Rechtsträger des betroffenen Unternehmens idR als personenbezogen iSd DSG darstellen. Die zu schützenden vertrauliche Daten werden dabei iE sowohl gem § 84 AktG als auch gem § 24 GmbHG als Teilmenge der nach § 1 DSG geschützten Daten einzuordnen sein.[268]

Aber auch Daten betreffend Mitarbeiter oder Mitgliedern von Führungsorganen der Gesellschaften können durch gesellschaftsrechtliche Bestimmungen zur Geheimhaltung geschützt sein.

Va in Hinblick auf die im Vorfeld von Umstrukturierungen regelmäßig durchgeführten Due Diligence Prüfungen sind die gesellschaftsrechtlichen Bestimmungen zum Geheimnisschutz von eminenter Bedeutung. Eine eingehende Untersuchung der Fragestellungen iZm derartigen Prüfungen erfolgt daher im entsprechenden Kap dieser Arbeit.[269]

---

[266] § 277 UGB.
[267] §280 UGB.
[268] *Doralt/Nowotny/Kalss*, Aktiengesetz (2003) § 84 Rz 15; iglS *Feltl/Mosing*, Das Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 237.
[269] S Kap V.E.

7. Datenschutz durch Wettbewerbsrecht

Behandelt man das Thema Datenschutz unter einem wettbewerbsrechtlichen Gesichtspunkt, geht es va um den Schutz und die Bedeutung solcher markt- bzw unternehmensbezogener Informationen, die sich auf das Wettbewerbsverhalten (bzw das mangelnde Wettbewerbsverhalten) von Unternehmen beziehen.[270] Entsprechend der Zielsetzung dieser Arbeit wird im Folgenden nur der Schutz jener Informationen/Daten behandelt, bei denen das Unternehmen als Betroffener iSd § 4 Z 3 DSG in Betracht kommen kann. Hierbei besonders interessierend ist der Schutz von Geschäfts- und Betriebsgeheimnissen.

a) Der Schutz personenbezogener Daten durch § 11 UWG

Diesen bezweckt va die Bestimmung des § 11 UWG.[271] Da das unternehmerische Geheimwissen nicht selten einen erheblichen wirtschaftlichen Wert hat, von dem insb auch die Überlebensfähigkeit eines Unternehmen abhängen kann, sucht § 11 UWG zu verhindern, dass Dritte durch die Kenntnis oder Verwertung fremder Geschäfts- und Betriebsgeheimnisse einen ungerechtfertigten Wettbewerbsvorteil realisieren.[272]

Die Bestimmung setzt sich bei näherer Betrachtung aus drei Tatbeständen zusammen: erstens dem Treuebruch durch einen Bediensteten während des aufrechten Dienstverhältnisses, zweitens der Verwertung von Geschäfts- oder Betriebsgeheimnissen sowie drittens der Mitteilung solcher Geheimnisse in Form der Betriebsspionage durch Betriebsfremde. [273]

Das Gesetz unterscheidet zwischen Geschäfts- und Betriebsgeheimnissen; mit ersteren sind Informationen technischer, mit letzterer kaufmännisch-geschäftlich Natur gemeint. Eine genaue begriffliche Unterscheidung scheint jedoch nicht erforderlich, da die Rechtsfolgen identisch sind.[274]

---

[270] Vgl *Thyri*, Geheimnisschutz-Datenschutz-Informationsschutz im Wettbewerbsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 217.
[271] § 11 Abs 1 UWG.
[272] *Koppensteiner*, Österreichisches und europäisches Wettbewerbsrecht[3] (1997) 588 Rz 1.
[273] *Koppensteiner*, Österreichisches und europäisches Wettbewerbsrecht[3] (1997) 587 Rz 1.
[274] *Koppensteiner*, Österreichisches und europäisches Wettbewerbsrecht[3] (1997) 589 Rz 5.

b) Bewertung der unternehmensbezogenen Relevanz

Meiner Auffassung nach bietet das UWG iVm mit den einschlägigen Bestimmungen des DSG va bei Verstößen gegen den Datenschutz taugliche Mittel zu einer entsprechenden Sanktionierung. § 11 UWG stellt im Gegensatz zu § 52 DSG nämlich unmittelbar nur auf den Verrat und das Verbreiten von Geschäfts- und Betriebsgeheimnissen ab, nicht jedoch auf deren Auskundschaften zum Zweck der Verwertung;[275] insofern ergänzen sich die Vorschriften.

Werden zB gesetzliche Vorschriften wie jene des DSG schuldhaft verletzt um sich einen Vorsprung gegenüber dem Mitbewerber zu verschaffen, steht diesem die Möglichkeit offen, auf Unterlassung und Schadenersatz[276] zu klagen; vorausgesetzt der Verstoß war geeignet den Leistungswettbewerb zu beeinträchtigen.[277]

Ganz grds kommen neben Geheimnisverletzungen iSd § 11 UWG freilich auch andere unlautere Geschäftspraktiken als klagslegitimierend in Betracht.[278] Die möglichen Konsequenzen eines solch schadenersatzrechtlichen Verfahrens werden sich dabei mE für das den Datenschutz verletzende Unternehmen finanziell oft bedrohlicher darstellen als die (bezüglich ihrer Höhe zT als „zahnlos“ empfunden) Sanktionen nach dem DSG.

8. Die Verarbeitung personenbezogener Daten als Geschäftsinhalt und deren Reglementierung

a) § 151 GewO

§ 151 GewO richtet sich an Adressverlage und Direktmarketingunternehmen und stellt sich als lex specialis zum DSG dar.[279] Die Norm enthält dabei datenschutzrechtliche Sonderbestimmungen in Form von Ausübungsvorschriften.[280]

---

[275] *Dohr/Pollirer/Weiss,* DSG[2] I (2002) § 11 UWG Anm 3.
[276] Vgl § 1 Abs 1 UWG.
[277] *Knyrim,* Datenschutzrecht (2003) 244.
[278] Zu denken ist bspw an unerlaubte Werbemaßnahmen im Bereich des E-Commerce; vgl Kap IX.
[279] *Kinscher,* GewO[13] (2007) 305.
[280] *Hanusch,* Kommentar zur GewO (2004) § 151 Rz 1.

Sowohl Adressverlage als auch Direktmarketingunternehmen betreiben Werbung, die sich direkt an ausgewählte Zielgruppen richtet.[281] Auch das Vermitteln von Kunden- und Interessentendateien zwischen den Inhabern und Nutzern solcher Interessentendateien gehört zum Geschäftsfeld dieser Unternehmen.[282] Grundlage dieser als Listbroking bezeichneten Tätigkeit ist das prinzipielle Recht jedes Gewerbetreibenden, Daten zu ermitteln und zu verarbeiten um Werbeaktionen durchzuführen.[283]

Insb Unternehmen bedienen sich für ihre Werbemaßnahmen gerne solcher Listen, da sich diese, je nach Zielgruppe, für gewöhnlich bereits in der Praxis (einerseits wurden die Listen im Normalfall bereits durch den Vermieter selbst benutzt, andererseits haben möglicherweise auch schon weitere Unternehmen die Listen gemietet und verwendet) bewährt haben.[284]

§ 151 Abs 3 enthält die Voraussetzungen unter denen ein Ermitteln personenbezogener Daten zulässig ist; die Verwendung der solcherart ermittelten Daten ist dabei immer auf die Dienstleistungserbringung des Marketings oder Werbemittelversands für Dritte oder auf das bloße Vermitteln von Dateien (Listbroking) beschränkt.[285]

An sich ist für jede Verarbeitung personenbezogener Daten die Zustimmung des Betroffenen erforderlich, § 151 Abs 5 GewO enthält diesbezüglich jedoch eine Ausnahme: Soweit keine Zustimmung der Betroffenen gem § 4 Z 14 DSG vorliegt, ihre Daten für Marketingzwecke Dritter zu übermitteln, dürfen Adressverleger und Direktmarketingunternehmer aus einer Kunden- und Interessentendatei nur ganz bestimmte Daten ermitteln.[286]

Voraussetzung für ein solche Datenermittlung ist jedoch stets, dass der Inhaber der Datei dem Adressverlag oder Direktmarketingunternehmen gegenüber schriftlich unbedenklich erklärt hat, dass die Betroffenen in geeigneter Weise über die Möglichkeit

---

[281] *Brandl/Hohensinner*, Datenschutzrechtliche Aspekte der Tätigkeit von Adressverlagen und Direktmarketingunternehmen, ecolex 2003, 135.
[282] § 151 Abs 2 GewO.
[283] *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 2.
[284] *Riegler*, Rechtskonforme Übermittlung von Kundendaten, 39.
[285] Vgl *Knyrim*, Datenschutzrecht (2003) 217.
[286] Siehe dazu die Aufzählung in § 151 Abs 5 GewO; mwN *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 6.

informiert wurden, die Übermittlung ihrer Daten für Marketingzwecke Dritter zu untersagen und dass eine solche Untersagung nicht erfolgt ist.[287]

In Bezug auf die Verwendung sensibler Daten[288] ist § 151 Abs 4 GewO beachtlich: Im Gegensatz zu der in § 4 Z 14 DSG vorgesehenen Zustimmung, die der Betroffene nur bei Kenntnis der Sachlage für den konkreten Fall erteilen kann, ist es diesem nunmehr im Rahmen einer Einwilligung[289] möglich (auch wenn ihm nur bekannt ist, dass die Daten von irgendeinem nicht näher genannten Direktmarketingunternehmen zu Marketingzwecken verwendet werden) rechtsgültig sein Einverständnis zur Verwendung seiner Daten zu erklären.[290]

Die Formulierung dieser Sonderbestimmung beruht va auf dem Umstand, dass gerade bei der Ermittlung von Marketingdaten durch Adressverlage und Direktmarketingunternehmen die Identität künftiger Nutzer vielfach nicht bekannt sein wird. Damit würde aber die, für eine nach dem strengen Regime des DSG wirksame Zustimmung erforderliche, „Kenntnis der Sachlage für den konkreten Fall“ iE eine unüberwindbare Hürde darstellen.[291] Ausgenommen von dieser speziellen rechtlichen Konstruktion bleiben jedoch strafrechtlich relevante Daten[292], die weiterhin nur bei Vorliegen einer Zustimmung gem § 4 Z 14 DSG verwendet werden dürfen.

Nach § 151 Abs 7 GewO müssen Adressverlage und Direktmarketingunternehmen Aussendungen im Zuge von Marketingaktionen, die sie mit von ihnen zur Verfügung gestellten oder von ihnen vermittelten Daten durchführen, so gestalten dass durch entsprechende Kennzeichnung des ausgesendeten Werbematerials die Identität der Auftraggeber jener Dateien, mit deren Daten die Aussendung adressiert wurde nachvollziehbar ist.[293]

---

[287] § 151 Abs 5 2. Satz GewO.
[288] § 4 Z 2 DSG.
[289] § 151 Abs 4 1. Satz GewO.
[290] *Brandl/Hohensinner*, Datenschutzrechtliche Aspekte der Tätigkeit von Adressverlagen und Direktmarketingunternehmen, ecolex 2003, 137.
[291] Vgl *Kinscher*, GewO[13] (2007) 308.
[292] § 8 Abs 4 DSG.
[293] Für die datenschutzrechtliche Pflicht zur Offenlegung des Auftraggebers vgl § 25 DSG.

Adressverlage und Direktmarketingunternehmen, die die Aussendung mit von ihnen zur Verfügung gestellten oder von ihnen vermittelten Daten selbst durchgeführt haben, sind grds zur Auskunft nach § 26 DSG verpflichtet.

Dies jedoch mit der Privilegierung, dass sie nur dann verpflichtet sind über die Aufraggeber der Ursprungsdateien Auskunft zu erteilen, wenn der Betroffene sein Auskunftsbegehren binnen drei Monaten nach der entsprechenden Werbesendung an den Adressverlag oder das Direktmarketingunternehmen gerichtet hat. Zudem muss die Auskunftserteilung auch nur anhand der vom Betroffenen zur Verfügung gestellten Informationen über die Werbeaussendung erfolgen.[294]

Jeder Betroffene hat ein Recht auf Löschung seiner Daten, die der Adressverleger und Direktmarketingunternehmer über ihn für Marketingaktionen gespeichert hat (diesem muss binnen acht Wochen kostenlos entsprochen werden).[295] Wenn der Betroffene nicht auf der physischen Löschung seiner Daten besteht, nachdem er über die möglichen Folgen einer solchen Löschung informiert worden ist, muss der Adressverleger und Direktmarketingunternehmer die Daten nur so sperren, dass sie nicht mehr für Marketingzwecke verwendet werden können.[296]

b) Bewertung der unternehmensbezogenen Relevanz

Die Bestimmung des § 151 GewO ist jedenfalls eine zentrale Norm iZm der unternehmerischen Nutzung von personenbezogenen Daten und im oa Geschäftsfeld daher von unbestritten großer Bedeutung.

Auch ist auf die sog „Robinson“-Liste nach § 151 Abs 9 GewO hinzuweisen, die durch den Fachverband Werbung und Marktkommunikation der Bundessparte „Gewerbe, Handwerk, Dienstleistung“ der Wirtschaftskammer Österreich geführt wird und in die sich Personen kostenlos eintragen lassen können, die die Zustellung von adressiertem Werbematerial für sich ausschließen wollen.[297] Werbesendungen die an keine konkrete

[294] *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 10.
[295] § 151 GewO Abs 8.
[296] *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 12.
[297] *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 13.

Adresse versandt werden[298] können jedoch auch durch Eintragung in die Liste nicht verhindert werden.[299]

Nicht zuletzt besteht für Unternehmen auch die Möglichkeit ihre eigenen Kundendaten nicht nur für eigene Werbezwecke zu verwenden, sondern diese wiederum selbst an Adressverlage und Direktwerbeunternehmen zu verkaufen.

Dies ist gem § 151 Abs 10 GewO jedoch nur dann zulässig, wenn sie die Betroffenen in geeigneter Weise darüber informiert haben, dass sie die Verwendung dieser Daten für Marketingzwecke Dritter untersagen können, und wenn keine Untersagung erfolgt ist.[300]

Wie die letzten Bsp gezeigt haben wird für Unternehmen va die Einhaltung der Informationspflichten bedeutsam sein; die Sicherstellung eines datenschutzkonformen Vorgehens durch eine entsprechende unternehmensinterne Organisation wird mE daher jedenfalls angezeigt sein.

9. Der Schutz personenbezogener Daten durch das Berufsgeheimnis

Im Folgenden werden nun zwei Berufsgeheimnisse exemplarisch dargestellt denen gerade bei gesellschaftsrechtlichen Umstrukturierungen große Bedeutung zukommen kann.

a) § 38 BWG als bereichspezifisches Berufsgeheimnis

Nach § 38 BWG dürfen Kreditinstitute, ihre Gesellschafter, Organmitglieder, Beschäftigte sowie sonst für Kreditinstitute tätige Personen Geheimnisse, die ihnen ausschließlich auf Grund der Geschäftsverbindungen mit Kunden oder auf Grund des § 75 Abs 5 BWG anvertraut oder zugänglich gemacht worden sind, nicht offenbaren oder verwerten.[301]

---

[298] IdZ wird etwa an sog „Postwurfsendungen“ zu denken sein.
[299] *Knyrim*, Datenschutzrecht (2003) 219.
[300] *Hanusch*, Kommentar zur GewO (2004) § 151 Rz 14.
[301] *Oppitz*, Bankgeheimnis, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 270.

Das Bankgeheimnis stellt den besonderen Fall eines Berufsgeheimnisses im Verfassungsrang[302] dar und bedeutet va eine Verpflichtung zur Geheimhaltung von Kundengeheimnissen.[303] Dem Geheimnisschutz unterliegen dabei alle Tatsachen, Vorgänge und Verhältnisse tatsächlicher und rechtlicher Natur, die nur einem verhältnismäßig engen Personenkreis bekannt und nach dem Interesse desjenigen, auf den sich das Geheimnis bezieht, nicht über diesen Kreis hinaus bekannt werden sollen.[304] Darunter sind ebenso Geschäfts- und Betriebsgeheimnisse wie das Bestehen von Vertrags- und sonstigen Rechtsverhältnissen und deren Inhalt zu verstehen.[305]

Aus datenschutzrechtlicher Perspektive ist zunächst festzuhalten, dass § 38 BWG grds auch einen Schutz des Persönlichkeitsbereiches des Einzelnen bezwecken kann.[306] Primär erfasst sind jedoch va Daten mit Vermögens- und weniger Personenbezug;[307] letztere können in Ausnahmefällen jedoch ebenfalls dem Bankgeheimnis unterliegen (so zB die Informationen über eine bevorstehende Scheidung im Zuge eines Anlageberatungsgespräches).

Generell bestehen Datenschutz und Bankgeheimnis nebeneinander, insb findet sich in § 15 Abs 1 DSG die Verpflichtung für Auftraggeber, Dienstleister und ihre Mitarbeiter, Daten aus Datenanwendungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten (wie eben bspw dem Bankgeheimnis nach § 38 BWG), geheim zu halten.[308] § 15 DSG begründet somit ex lege eine eigene berufliche Geheimhaltungspflicht.[309]

§ 38 Abs 2 BWG normiert jene Ausnahmefälle in denen keine Verpflichtung zur Wahrung des Bankgeheimnisses besteht.[310] Bei Vorliegen der dort genannten Voraussetzungen entfällt nicht nur die Verpflichtung zur Geheimhaltung, sondern es ist

---

[302] § 38 Abs 5 BWG.
[303] *Sommer/Hirsch* in *Dellinger*, Bankwesengesetz (2007) § 38 Rz 2.
[304] *Laurer*, Bankwesenwesengesetz[3] (2008) § 38 Rz 3; mwN *Oppitz*, Bankgeheimnis, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 271.
[305] *Sommer/Hirsch* in *Dellinger*, Bankwesengesetz (2007) § 38 Rz 32.
[306] *Sommer/Hirsch* in *Dellinger*, Bankwesengesetz (2007) § 38 Rz 10.
[307] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 38 BWG Anm 1.
[308] *Oppitz*, Bankgeheimnis, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg)* Geheimnisschutz Datenschutz Informationsschutz (2008) 272.
[309] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 170.
[310] S *Dohr/Pollirer/Weiss*, DSG[2] (2002) Anh V/1/D § 38 BWG Anm 4.

auch die Berufung auf das Bankgeheimnis unzulässig (soweit Aussage- und Offenlegungspflichten zum Zug kommen).[311]

Gem. § 38 Abs 5 BWG können die Abs 1 bis 4 der Bestimmung vom Nationalrat nur unter erschwerten Bedingungen abgeändert werden (erforderlich ist eine Verfassungsmehrheit, wonach zumindest die Hälfte der Abgeordneten anwesend sein muss und mindestens zwei Drittel der Abgeordneten der Änderungen zustimmen müssen) woraus nicht zuletzt die besondere Bedeutung des Bankgeheimnisses im österreichischen Wirtschaftsrecht deutlich wird.[312]

b) § 91 WTBG

Als bei Unternehmensumstrukturierungen bedeutende spezifische berufliche Geheimhaltungspflicht soll schließlich auch die Bestimmung des § 91 WTBG kurz dargestellt werden. Wirtschaftstreuhänder werden aufgrund ihrer betriebswirtschaftlichen Kompetenz (zB als unabhängige Sachverständige)[313] häufig im Rahmen von Due Diligence Prüfungen tätig und gelangen somit naturgemäß an eine Vielzahl von Wirtschaftsdaten, weshalb sich gerade hierbei ein funktionierender Schutz dieser für das Unternehmen äußerst wichtigen Informationen als unerlässlich erweist.

Die Verschwiegenheitspflicht stellt die rechtliche Grundlage zur Schaffung und Absicherung des besonderen Vertrauensverhältnisses zwischen Mandant und Wirtschaftstreuhänder dar. Der sachliche Geltungsbereich erstreckt sich dabei nicht nur auf ausdrücklich anvertraute Angelegenheiten, die dem Wirtschaftstreuhänder im Zuge seiner beruflichen Tätigkeit zur Kenntnis gelangen, sondern auch auf jene die ihm lediglich „bekannt“ geworden sind. Ein explizites Anvertrauen mittels aktiver Information durch den Mandanten ist somit nicht erforderlich.[314]

---

[311] Die in § 38 Abs 2 BWG vorgenommene Aufzählung von Ausnahmetatbeständen ist nach der hL lediglich demonstrativ; mwN *Sommer/Hirsch* in *Dellinger*, Bankwesengesetz (2007) § 38 Rz 161.
[312] *Laurer*, Bankwesenwesengesetz[3] (2008) § 38 Rz 27.
[313] Vgl *Krejci*, Verschwiegenheitspflicht des AG-Vorstands bei Due-Diligence-Prüfungen, RdW 1999, 574; *Nowotny*, „Due Diligence“ und Gesellschaftsrecht, WBl 1998, 145; mwN *Hofman*, Due Diligence – Grenzen und Möglichkeiten des Managements (2006) 167.
[314] *Bernbacher/Haase/Herneth/Klement/Trojer* (Hrsg), Wirtschaftstreuhandberufsgesetz (2000) 117.

Weiters besteht ein Verbot der unbefugten Verwertung von Geschäfts- und Betriebsgeheimnissen, die unter die Verschwiegenheitspflicht fallen. Der Wirtschaftstreuhänder muss dafür sorgen, dass Unbefugte während und nach Beendigung der Tätigkeit keinen Einblick in Mandantenunterlagen und Mandanten betreffende Unterlagen haben. Mitarbeiter, Gesellschafter und Aufsichtsräte sind gleichfalls zur Verschwiegenheit verpflichtet und hierüber auch entsprechend zu belehren.[315]

c) Bewertung der unternehmensbezogenen Relevanz

Der grundlegenden Zielsetzung des BWG als Wirtschaftsaufsichtsgesetz entsprechend, ist die praktische Bedeutung für den unternehmerischen Bereich entsprechend groß.[316] So wird bei der Verwendung personenbezogener Daten im Rahmen der Umstrukturierung von Banken regelmäßig der verfassungsrechtlich gewährleistete Schutz des Bankgeheimnisses neben den datenschutzrechtlichen Vorschriften zu beachten sein.

Insb im Rahmen von Due Diligence Prüfungen können sich im Spannungsfeld zwischen dem umfassenden Informationsbedürfnisses des Kaufinteressenten und dem durch das Bankgeheimnis gewährleisteten Geheimnisschutz zahlreiche Fragen stellen.[317] Zur Generierung der akquisitionsrelevanten Informationen werden dabei regelmäßig Sachverständige wie bspw Rechtsanwälte und eben auch Wirtschafstreuhänder herangezogen.

Insofern stellt sich daher auch das WTBG als ein gerade bei Unternehmensprüfungen typischerweise beachtliches Gesetz dar, dem in der wirtschaftlichen Praxis eine dementsprechend große Beachtung zu Teil werden muss.

---

[315] *Bernbacher/Haase/Herneth/Klement/Trojer* (Hrsg), Wirtschaftstreuhandberufsgesetz (2000) 118;
[316] MwN *Oppitz*, Bankgeheimnis, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 275.
[317] Vgl *Nowotny*, „Due Diligence“ und Gesellschaftsrecht, WBl 1998, 145.

10. Die DSG-Novelle 2010

Nachdem mit der DSG-Novelle 2008[318] bereits einmal ein Versuch zur Novellierung des DSG unternommen wurde, dieser jedoch ua aufgrund einer Regierungsumbildung nicht zustande kam, wurden schließlich mit der DSG-Novelle 2010[319] einige Änderungen im Regime des DSG herbeigeführt.

Im Folgenden kann und soll nun keine ausführliche Diskussion der einzelnen Änderungen geboten werden, vielmehr soll gezielt auf jene Aspekte der Nov hingewiesen werden, die va im unternehmerischen Zusammenhang von Bedeutung sein können.

a) Überblick über die wichtigsten Änderungen

Kernpunkte der Novelle sind die Regelungen über die Videoüberwachung, die Bündelung der datenschutzrechtlichen Kompetenzen beim Bund, sowie ein vereinfachtes Anmeldeverfahren beim DVR.[320]

Besonders Letzteres war in Anbetracht der stetig steigenden Belastung des DVR erklärtes Ziel der Nov; das DVR soll künftig in Form einer Datenbank geführt und Meldungen primär in automationsunterstützter Form über eine Internetanwendung (online) erstattet werden, damit die Verwaltungsabläufe vereinfacht und beschleunigt werden können.[321]

Im Vergleich zum ersten Entwurf wurde weiters von einer Einschränkung des Datenschutzes auf natürliche Personen Abstand genommen, womit iE nun weiterhin auch Unternehmen als juristische Personen den Schutz des DSG genießen. Auch auf die Erhöhung der Sanktionen nach § 52 DSG bei Datenschutzverstößen auf € 25.000,-- bzw € 10.000,-- ist hinzuweisen.[322]

---

[318] ME DSG-Novelle 2008, 182/ME 23. GP.
[319] ME DSG-Novelle 2010, 62/ME 24. GP; die Begutachtungsfrist für die DSG-Novelle 2010 endete mit 17.6.2009, es ist insofern davon auszugehen, dass der Entwurf weitgehend in seiner derzeitigen Fassung in Geltung tritt.
[320] Vgl dazu *Kunnert*, Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009, 102.
[321] S dazu 62/ME 24. GP Mat 7.
[322] 62/ME 24. GP Mat 13.

Nicht mehr enthalten ist schließlich die Bestimmung betreffend eines betrieblichen Datenschutzbeauftragten.[323]

b) Bewertung der unternehmensbezogenen Relevanz

Zum gegenwärtigen Zeitpunkt kann mangels jeglicher Erfahrungswerte freilich nur eine allererste Einschätzung der künftigen Auswirkungen der DSG-Novelle 2010 gegeben werden.

Vorrangig ist die Beibehaltung des Grundrechtsschutzes auch für juristische Personen zu begrüßen, Unternehmen bzw deren Rechtsträger sind bezüglich ihrer personenbezogenen Daten somit weiterhin durch das DSG geschützt.[324] Ein Umstand, der va bei den betroffenen Unternehmen auf ein durchwegs positives Echo gestoßen ist.[325] Neben anderen einfachgesetzlichen Bestimmungen besteht ein unternehmerischer Geheimnisschutz somit weiterhin auch im Verfassungsrang; kraft der unmittelbaren Drittwirkung kann der Anspruch auf Geheimhaltung daher va gegebenenfalls auch im Verhältnis zwischen konkurrierenden Unternehmen geltend gemacht werden.[326]

Weiters wird sich mE va die nunmehr in rein elektronischer Form abzuwickelnde Registrierung von Datenanwendungen als Vereinfachung im unternehmerischen Alltag darstellen. Die Änderung ist daher dementsprechend zu begrüßen.

Für größere Unternehmen bzw solche in Konzernstrukturen wird sich auch die Neuregelung zur Meldung des Betreibens eines Informationsverbundsystems als Erleichterung erweisen können. Künftig kann diese Verpflichtung vom Auftraggeber auf den Betreiber des Informationsverbundsystems übertragen werden.[327]

---

[323] So noch § 15a im Entwurf der DSG-Novelle 2008; s 182/ME 23. GP Mat 4.
[324] Dies ist für Unternehmen insofern von Bedeutung als eben auch wirtschaftliche Informationen wie Daten über Umsatz, Gewinn oder Verlust als personenbezogen iSd DSG zu beurteilen sind; s Kap IV.B.6.b).
[325] Vgl dazu etwa die Stellungnahmen der mobilkom austria AG (30/SN-62/ME 24.GP), der Österreichischen Post AG (51/SN-62/ME 24. GP) sowie auch der Industriellenvereinigung (34/SN-62/ME 24.GP bzw 41/SN-182/ME 23. GP) und der Wirtschaftskammer Österreich (24/SN-62/ME 24. GP) als unzweifelhaft wirtschaftliche bzw unternehmerische Interessenvertretungen.
[326] S Kap IV.A.1.d).
[327] Vgl § 50 Abs 2 DSG-Novelle 2010; s 62/ME 24. GP Mat 11.

Auch der Entfall des betrieblichen Datenschutzbeauftragten bedeutet für die Unternehmen iE ein Weniger (bzw das Unterbleiben) des diesbezüglichen organisatorischen Aufwandes.[328]

Zusammenfassend sind die durch die DSG-Novelle 2010 implementierten Neuerungen aus unternehmerischer Sicht meiner Auffassung nach durchaus zu begrüßen. Im Hinblick auf die Erhöhung der Verwaltungsstrafen nach § 52 DSG ist es mE jedoch nach wie vor zweifelhaft, ob die Bestimmung in Anbetracht der Höhe der Beträge tatsächlich präventiv wirken kann; diesbezüglich wird als Intention seitens des Gesetzgebers wohl eher von einer Betragsbereinigung als der Schaffung wirklich scharfer Sanktionen auszugehen sein.

Die generelle praktische Relevanz der Nov sowie auch noch etwaige auftauchende Fragestellungen idZ werden sich freilich erst im Laufe der Zeit erweisen können.

[328] IdS auch die Stellungnahme der Wirtschaftskammer Österreich (24/SN-62/ME 24. GP) und der Industriellenvereinigung (34/SN-62/ME 24. GP); den Entfall des betrieblichen Datenschutzbeauftragten massiv kritisierend dagegen die ARGE Daten (2/SN-62/ME 24. GP).

C. Datenschutz durch Selbstregulierung in der Wirtschaft

Abschließend soll neben den Bestimmungen des staatlichen Gesetzgebers noch auf die zunehmend autonome Entwicklung von den Datenschutz im Unternehmen betreffenden Regelungen seitens der Privatwirtschaft hingewiesen werden.

1. Privacy Policies

Insb im Bereich elektronischer Dienstleistungen durch grenzüberschreitend agierende Unternehmen kommt dem Phänomen der sog „Privacy Policies“ eine zunehmende Bedeutung zu. Darunter sind Erklärungen von Unternehmen über deren Datenschutzpolitik zu verstehen, deren Zweck darin liegt, den Kunden über die vom Unternehmen vorgenommene Datenverarbeitung aufzuklären und Verständnis für diese zu erwirken.[329]

Diese Datenschutzerklärungen haben sich zunächst in den USA und inzwischen weltweit (und in besonderem Ausmaß in Internet-Auftritten durchgesetzt). Der Ausgang aus dem amerikanischen Recht liegt va in einem grundlegend anderem Rechtsverständnis: Diesem zufolge hat der Datenschutz in erster Linie eine Abwehrfunktion und soll den Einzelnen vor Eingriffen durch den Staat schützen. Zum einen wird va auf Selbstregulierung (eben in Form unternehmenseigener Privacy Policies) vertraut, zum anderen soll eine Geltung unter Privaten (etwa vergleichbar mit einer unmittelbaren Drittwirkung, wie im österr DSG angeordnet) vermieden werden.[330] Aus diesen Gründen wurde zwischen der EU und den USA auch schließlich ein eigenes Übereinkommen abgeschlossen (mehr dazu in Kap V.F.)

Inhaltlich werden in den jeweiligen Privacy Policies durchaus unterschiedliche Beschreibungen des Umgangs mit (personenbezogenen) Daten der Nutzer gegeben. Urheber ist das Unternehmen selbst, wobei es vorerst noch keine unabhängige Kontrollstelle zur Überprüfung der jeweiligen Privacy Policy gibt. Mittlerweile gibt es jedoch zunehmend Bestrebungen (zB durch den von der OECD zur Verfügung

---

[329] *Knyrim*, Datenschutzrecht (2003) 186.

[330] *Genz*, Datenschutz in Europa und den USA (2004) 166; *Räther/Seitz*, Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 427.

gestellten „Privacy Statement Generator“)[331] diese Datenschutzerklärungen zu standardisieren, um eine nutzerfreundliche Vorauswahl datenschutzgerechter Internetauftritte zu gewährleisten.[332] Letztlich soll dadurch va eine vertrauensvolle Beziehung des Kunden zum Unternehmen geschaffen werden.[333]

Besonders die Datenschutzrichtlinie für die elektronische Kommunikation[334] leistet dieser Entwicklung dadurch Vorschub, dass Unternehmen die Verwendung sog „Cookies“ (darunter sind Textdateien zu verstehen, in denen ein Webserver Informationen über den Surfer auf dessen PC abspeichert und beim nächsten Besuch der Seite von dort wieder abruft)[335] gestattet ist[336], sofern die Nutzer oder Kommunikationsteilnehmer darüber entsprechend informiert werden.[337]

Um einer solchen Informationspflicht nachzukommen bieten Privacy Policies für Unternehmen ein denkbar taugliches Instrument, weshalb mit einer noch weiter wachsenden Bedeutung dieses Rechtsgebiets in naher Zukunft zu rechnen ist.

2. Codes of Conduct

Datenschutz durch Selbstregulierung kann weiters auch durch sog Codes of Conduct vorgenommen werden, mit denen die Unternehmen eine Selbstverpflichtung konstituieren. Unter diesem Begriff sind Verhaltensregeln zu verstehen, denen sich ein Unternehmer unterwirft, um durch Selbstregulierung zu bereichsspezifischen Regelungen zu kommen, die eine möglicherweise übermäßige gesetzgeberische Aktivität in diesem Bereich erspart.[338]

---

[331] http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html (16.11.2008).
[332] *Simitis*, dBDSG[6] (2006) § 33 Rz 42.
[333] *Salmen/Ruhland*, Elektronische Marketingkampagnen: Zwischen E-Privacy und Electronic Customer Care, ÖBA 2003, 533.
[334] Vgl Kap I.A.2.
[335] http://www.internet4jurists.at/intern27.htm (17.11.2008).
[336] Vgl dazu Art 5 Abs 3 RL 2002/58/EG.
[337] *Jahnel*, Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, WBl 2003, 108.
[338] *Gola/Schomerus*, dBDSG[9](2007) § 38 a Rz 2; vgl dazu auch *Patzak*, Datenschutzrecht für den E-Commerce (2004) 515.

Insb im internationalen (und dabei va dem Us-amerikanischen) Wirtschaftskreis ist man bereits dazu übergegangen, Netzwerke von Unternehmen zu gründen, die sich ihre eigenen Datenschutzregeln im Rahmen der gesetzlichen Vorgaben geben.[339]

Hinzweisen ist idZ auch auf den Global Business Dialog on Electronic Commerce[340] in dem sich zahlreiche Unternehmen zusammengeschlossen haben, um weltweit geltende Regeln für den elektronischen Geschäftsverkehr zu entwickeln. Auf seinem mittlerweile zehnten Gipfel (am 31.10.2008 in San Francisco) wurden ua Empfehlungen in den Bereichen digitales Heim, NFC-Payments[341] sowie Internetsicherheit verabschiedet.[342]

Ob sich jedoch die mannigfachen datenschutzrechtlichen Fragestellungen im Wege der Selbstregulierung (allein) lösen lassen ist meiner Auffassung nach zumindest fraglich. Dem Erfordernis einer angemessenen Interessensabwägung zwischen datenverarbeitenden Unternehmen und den hiervon betroffenen Personen wird eine ausschließlich privatautonome Regelung schon auf Grund des ökonomischen Ungleichgewichts idR nicht gerecht werden können.

Abgesehen davon zeigt zumindest der österr Weg der Implementierung eines Grundrechts auf Datenschutz den besonderen Stellenwert des Rechts auf informationelle Selbstbestimmung in der nationalen Rechtsordnung. Insofern kann ein durch private Vereinbarungen begründetes datenschutzrechtliches Regime für den Betroffenen keinesfalls einem Schutz im Rahmen eines verfassungsgesetzlich gewährleisteten Rechts gleichkommen.

Va der europäische Gesetzgeber hat in Anbetracht seiner Kompetenzen vielmehr die Verpflichtung einen entsprechenden gesetzlichen Rahmen für die unternehmerische Selbstregulierung zu schaffen. Die von den Unternehmen solcherart erlassenen Codes of Conduct sind dann in weiterer Folge von den staatlichen Kontrollbehörden auf ihre Vereinbarkeit mit den gesetzlichen Regelungen zum Datenschutz zu prüfen und gegebenenfalls anzuerkennen.[343]

---

[339] Vgl Kap V.F.3.b)(2).
[340] http://www.gbd-e.org/about.html (31.3.2009).
[341] Sog Near Field Communication (idZ eingesetzt zur kontaktlosen Zahlung via Mobiltelefon).
[342] http://www.gbd-e.org/publications.html (31.3.2009).
[343] IglS *Patzak*, Datenschutzrecht für den E-Commerce (2004) 515.

Im Folgenden wird nun eine Darstellung jener unternehmerischer Bereiche geboten, aus denen sich datenschutzrechtliche Implikationen ergeben können. Dabei können sowohl externe wirtschaftliche Transaktionen als auch rein unternehmensinterne Abläufe datenschutzrechtlich relevante Sachverhalte darstellen.

V. Gesellschaftsrechtliche Umstrukturierungen des Unternehmens

A. Begriff und Formen der Unternehmensumstrukturierung

Dem Begriff der Umstrukturierung (bzw auch dem der Umwandlung) wird im Wirtschaftsleben allgemein eine umfassende Bedeutung beigemessen. Im weitesten Sinn kann darunter jede gesellschaftsrechtliche Änderung der Struktur eines Rechtsträger verstanden werden.[344]

Einen derart universellen Begriffsinhalt verwendet auch das dUmwG[345]. § 1 dUmwG nennt taxativ vier zulässige Umwandlungsarten: die Verschmelzung, die Spaltung, die Vermögensübertragung und den Formwechsel.

In der älteren österr Lit[346] findet sich dagegen eine scheinbar engere Auslegung des Umwandlungsbegriffs; als Umwandlung wird dabei grds ein Vorgang bezeichnet, bei dem ein Unternehmen seine Rechtsform ändert. Dadurch kann jedoch der Eindruck entstehen, dass nur die Änderung des äußeren Erscheinungsbildes eines Rechtsträgers im Sinne einer formändernden Umwandlung ausgelegt wird. Tatsächlich wird als Umwandlungsvorgang aber nicht nur die formändernde Umwandlung, sondern auch die übertragende Umwandlung verstanden, bei der das Gesellschaftsvermögen im Wege der Gesamtrechtsnachfolge auf einen anderen Rechtsträger übergeht.[347]

In der Folge sind unter dem Begriff der Umstrukturierung va Verschmelzungen, Spaltungen und Umwandlungen ieS zu verstehen. Ein Schwerpunkt wird nunmehr auf die Umstrukturierungsmaßnahmen der Verschmelzung und Spaltung gelegt, da bei diesen Vorgängen erfahrungsgemäß die meisten datenschutzrechtlichen Fragen auftreten.

Der eingehenderen Behandlung vorangestellt wird eine kurze Definition und Erläuterung der gegenständlichen Umstrukturierungsmaßnahmen.

---

[344] Vgl dazu auch *Torggler*, Umgründung, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 311.
[345] Umwandlungsgesetz vom 28. Oktober 1994, dBGBl I, 3210.
[346] *Kotrnoch*, Steuerfragen zur Umwandlung von Kapitalgesellschaften, in FS Helbich (1990) 81.
[347] MwN *Schummer* in *Helbich/Wiesner/Bruckner (Hrsg)*, Handbuch der Umgründungen (2002) Allgemein Bemerkungen Rz 1.

1. Verschmelzung

Unter einer Verschmelzung (oder auch Fusion) ist die Vereinigung der Vermögen von zwei oder mehreren Gesellschaften[348] im Wege der Gesamtrechtsnachfolge gegen Gewährung von Anteilen der übernehmenden Gesellschaft an die Gesellschafter der übertragenden Gesellschaft(en) zu verstehen.[349]

Dabei lassen sich zwei Varianten unterscheiden: Die Verschmelzung durch Aufnahme und die Verschmelzung durch Neugründung. Im ersten Fall wird das Vermögen einer (oder mehrerer) übertragenden(r) Gesellschaft auf eine übernehmende Gesellschaft übertragen, im zweiten Fall wird das Vermögen zweier oder mehrerer Gesellschaften auf eine neu zu bildende Gesellschaft übertragen.[350]

Die Verschmelzungen von Gesellschafen mbH ist in den §§ 96 ff GmbHG geregelt, jene einer GmbH mit einer AG in § 234 AktG und die Verschmelzung mehrerer AG miteinander in den §§ 219 ff AktG.[351]

2. Spaltung

Unter einer Spaltung ist die Übertragung von Teilen des Vermögens einer (übertragenden) Gesellschaft auf eine oder mehrere andere Gesellschaften auf gesellschaftsrechtlicher Grundlage gegen Gewährung von Anteilen der empfangenden Gesellschaft(en) an die Gesellschafter der übertragenden Gesellschaft zu verstehen.[352]

Eine derartige Vermögensspaltung ist grds in zwei Formen möglich: Zum einen als Aufspaltung; diese ist durch die Auflösung der übertragenden (aufspaltenden)

---

[348] Vgl dazu auch *Rauter*; Verband, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 323, wo allgemein der Begriff „Verband" benutzt wird (da darunter jedoch auch jede rechtsfähige Gesellschaft zu verstehen ist, wird im Folgenden die Diktion „Gesellschaft" beibehalten).

[349] *Torggler*, Verschmelzung, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 332.

[350] *Koppensteiner/Rüffler* , GmbHG-Kommentar[3] (2007) § 96 Rz 2; *Mader*, Kapitalgesellschaften[6] (2008) 52; *Duursma/Duursma-Kepplinger/Roth*, Handbuch zum Gesellschaftsrecht (2007) Rz 3401; mwN *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 219 AktG Rz 2; zur begrifflich identen Rechtslage in D vgl *Semler/Stengel*, Kurzkommentar dUmwG § 2 Rz 22.

[351] *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 219 AktG Rz 5.

[352] *Torggler*, Spaltung, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 286; mwN *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) Vorbemerkungen zum SpaltG Rz 5.

Gesellschaft und den Übergang des gesamten Vermögens auf mehrere übernehmende Gesellschaften gekennzeichnet.
Zum anderen als Abspaltung, wobei diese dadurch charakterisiert ist, dass ein oder mehrere Vermögensteile auf eine oder mehrere Gesellschaften übertragen werden und die übertragende Gesellschaft dabei bestehen bleibt.[353]

Innerhalb der Auf- bzw Abspaltung kann weiters auf solche zur Neugründung oder solche zur Aufnahme unterschieden werden, je nachdem, ob der empfangende Verband bei der Spaltung bereits besteht oder erst gegründet wird.[354] Die rechtliche Grundlage für Spaltungen bildet das SpaltG[355].

3. Umwandlung

Umwandlungen sind schließlich in den §§ 239 ff AktG sowie im UmwG[356] geregelt. Als übertragende Umwandlung wird ein Sachverhalt verstanden, in dem das Vermögen einer Kapitalgesellschaft im Wege der Gesamtrechtsnachfolge übertragen wird, ohne dass die Gesellschaft dabei abzuwickeln ist.[357]

Hierbei kann zwischen einer verschmelzenden und einer errichtenden Umwandlung unterschieden werden: Die verschmelzende Umwandlung ist dadurch gekennzeichnet, dass das Vermögen auf den Hauptgesellschafter als Nachfolgerechtsträger, der bereits besteht und zumindest zu 90% an der umzuwandelnden Kapitalgesellschaft beteiligt ist, übergeht. Die errichtende Umwandlung zeichnet sich dagegen durch die Neugründung einer OG oder KG aus, auf die das Vermögen der Kapitalgesellschaft im Weg der Gesamtrechtsnachfolge (unter Ausschluss der Abwicklung) übergeht.[358] Sowohl die verschmelzende[359] als auch die errichtende[360] Umwandlung sind im UmwG geregelt.

---

[353] *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 1 SpaltG Rz 3.
[354] *Mader*, Kapitalgesellschaften[6] (2008) 55; *Torggler*, Spaltung, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 287.
[355] Bundesgesetz über die Spaltung von Kapitalgesellschaften (SpaltG), BGBl 1996/304 idF BGBl I 2008/70.
[356] Bundesgesetz über die Umwandlung von Handelsgesellschaften (UmwG), BGBl 1996/304 idF BGBl I 2007/72.
[357] *Mader*, Kapitalgesellschaften[6] (2008) 55.
[358] *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 1 UmwG Rz 4.
[359] §§ 2 bis 4 UmwG.
[360] § 5 UmwG.

Anders stellt sich die formändernde Umwandlung[361] dar, hierbei erfolgt lediglich eine Änderung der Rechtsform (von einer GmbH zu einer AG oder umgekehrt) ohne Vermögensübertragung;[362] mangels einer Gesamtrechtsnachfolge und der sich daraus ergebenden Fragen und Problemstellungen kann diese Form der Umwandlung iE als datenschutzrechtlich neutral betrachtet werden.[363]

Im Zuge der anschließenden Erörterung werden die jeweiligen Umstrukturierungen für GmbH und AG gemeinsam untersucht, da die datenschutzrechtlichen Fragestellungen weitgehend ident sind.

B. Die Gesamtrechtsnachfolge als Wesensmerkmal von Verschmelzung und Spaltung

Die Gesamtrechtsnachfolge stellt sich als gesetzlich determiniertes[364] Charakteristikum von Verschmelzung und Spaltung dar; beide Umstrukturierungsformen zeichnen sich durch eine Vermögensübertragung mittels Gesamtrechtsnachfolge aus.[365]

Im Gegensatz zur Verschmelzung nach den Bestimmungen der §§ 219 und 225a Abs 3 AktG stellt sich die Rechtsnachfolge bei der Spaltung jedoch nur partiell dar: Es geht dabei nur ein Teil des Vermögens des übertragenden Rechtsträgers auf einen bestimmten übernehmenden Rechtsträger über (der andere Teil verbleibt im Abspaltungsfalls beim übertragenden Rechtsträger bzw wird auf einen anderen übernehmenden Rechtsträger übertragen).[366]

Aus datenschutzrechtlicher Sicht ist die (als Rechtsinstitut ja durch den Identitätswechsel des Rechtsträgers zwingend erforderliche) Gesamtrechtsnachfolge bei den angeführten gesellschaftsrechtlichen Umstrukturierungsmaßnahmen ein ganz

---

[361] Vgl § 239 und § 245 AktG.
[362] *Torggler*, Umgründung, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006) 311; *Duursma/Duursma-Kepplinger/Roth*, Handbuch zum Gesellschaftsrecht (2007) Rz 4528; mwN *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) Vorbemerkungen zum UmwG Rz 1.
[363] Vgl dazu *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 12.
[364] § 219 Z 1 und Z 2 AktG; § 1 Abs 2 Z 1 und Z 2 SpaltG.
[365] *Jabornegg/Strasser*, Kommentar zum AktG[4] (2001) § 219 Rz 5; *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 234.
[366] *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 14 SpaltG Rz 8; *Duursma/Duursma-Kepplinger/Roth*, Handbuch zum Gesellschaftsrecht (2007) Rz 4425.

wesentliches Merkmal. Dies da hierdurch eine Übermittlung iSd § 4 Z 12 DSG[367] verwirklicht werden kann; idZ muss jedoch darauf hingewiesen werden, dass die Frage, ob eine solche im Rahmen der Umstrukturierung überhaupt vorliegt, str ist.[368] Eine eingehendere Untersuchung dieser Fragestellung erfolgt in Kap V.E.2.

C. Der datenschutzrechtliche Betroffenenbegriff bei Umstrukturierungsmaßnahmen - Arten von personenbezogenen Daten

Um eine Aussage über etwaige datenschutzrechtliche Implikationen im Zuge einer Umstrukturierung treffen zu können, müssen zunächst folgende „Akteure" nach dem Regime des DSG abgegrenzt werden: der Betroffene[369], der Auftrageber[370] und (falls vorhanden) der Dienstleister[371].

Dem grundrechtlichen Schutz des DSG sind immer nur solche Daten unterworfen, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht.[372] Bei der gesellschaftsrechtlichen Umstrukturierung eines Unternehmens kann grds zwischen personenbezogenen Daten, deren Schutz im Interesse der juristischen Person (dh dem Rechtsträger des umzustrukturierenden Unternehmens), der einzelnen Mitarbeiter sowie der Kunden des Unternehmens liegt unterschieden werden.[373]

Daraus folgt, dass bei Umstrukturierungen idR drei Gruppen von Betroffenen zu beachten sind: Erstens das Unternehmen als juristische Person selbst, zweitens die

---

[367] Leg cit, die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

[368] Dafür *Wengert/Widmann/Wengert*, Bankenfusionen und Datenschutz, NJW 2000, 1291; *Teichmann/Kiesling*, Datenschutz bei Umwandlungen, ZGR 2001, 52; *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 242; *Auer/Feltl*, Zur datenschutzrechtlichen Relevanz von Umstrukturierungsvorgängen, SWK 2009, 815; abl *Lüttge*, Unternehmensumwandlungen und Datenschutz, NJW 2000, 2465; *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 101.

[369] § 4 Z 3 DSG; leg cit, jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft deren Daten verwendet werden.

[370] § 4 Z 4 DSG; leg cit, natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft, bzw die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffenen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen.

[371] § 4 Z 5 DSG; leg cit, natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden.

[372] Vgl Kap IV.A.I.

[373] Vgl *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 235.

Mitarbeiter (bzw all jene Betroffenen die in einem aufrechten Vertragsverhältnis zum Unternehmen stehen)[374] und drittens Kunden des Unternehmens (als Betroffene deren personenbezogene Daten zwar einmal iZm der Erfüllung eines Vertrages dem Unternehmen bekanntgegeben wurden, die jedoch nun in keinerlei rechtlicher Beziehung mehr zum Unternehmen stehen).

Das Abstellen auf ein aufrechtes Vertragsverhältnis zum umzustrukturierenden Unternehmen ist mE deshalb zielführend, da sich im wirtschaftlichen Alltag für den Auftraggeber der Datenverarbeitung neben dem Vorliegen überwiegender Interessen nicht selten vertragliche Verpflichtungen als das am besten geeignete Instrument um iE zu einer Zulässigkeit der Verarbeitung zu kommen, darstellen werden.

Nachdem die einzelnen, im Zuge der Umstrukturierung Betroffenen iSd DSG herausgearbeitet wurden, wird nun untersucht welche Arten von personenbezogenen Daten dabei in Betracht kommen können.

1. Unternehmensdaten

Fraglich ist, welche Daten beim Unternehmen als juristische Personen personenbezogen iSd DSG sein können. Gem § 4 Abs 1 DSG sind unter dem Begriff der personenbezogenen Daten leg cit „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist“ zu verstehen.

Bei natürlichen Personen wird es sich hierbei va um Daten des Privat-, Familien- und Erwerbslebens handeln. Bspw also Name, Geburtsdatum und Geburtsort, Staatsangehörigkeit, Religionsbekenntnis, Familienstand, Adresse, Sozialversicherungsnummer, Angaben über bestimmte Kenntnisse und Fähigkeiten eines Menschen, Vermögen etc.[375]

[374] IdZ typischerweise im Rahmen eines Arbeitsverhältnisses.
[375] § 4 Z 1 DSG; *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 2; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 117.

Eine Definition personenbezogener Daten bei juristischen Personen kann dagegen auf den ersten Blick, nicht zuletzt mangels europarechtlicher Vorgaben[376], deutlich weniger leicht gegeben werden.

Unstrittig, da mittlerweile durch Rsp[377] wie Lit[378] hinlänglich herausgearbeitet, ist jedoch, dass Wirtschaftsdaten (zB Daten aus dem Kunden- und Lieferantenverkehr oder Geschäfts- und Betriebsgeheimnisse) als personenbezogene Daten juristischer Personen einzuordnen sind. Damit sind iE auch Daten über den Umsatz, Marktprognosen, betriebliche Logistik etc vom Schutz des DSG erfasst.

2. Mitarbeiterdaten

Auch Arbeitnehmer des Unternehmens sind bezüglich ihrer personenbezogenen Daten als Betroffene iSd DSG einzuordnen.[379] Neben den in Kap V.D.1. bereits aufgezählten Daten sind iZm einem Beschäftigungsverhältnis auch Daten wie Vergütungsgruppe, Personalnummer, Leistungsbeurteilungen und dgl (iE daher alle beim Unternehmen über seine Arbeitnehmer vorhandenen Informationen, die einem Geheimhaltungsanspruch zugänglich sind) personenbezogen iSd § 4 Abs 1 DSG.

Auch sensible Daten iSd § 4 Z 2 DSG sind dabei oftmals erfasst; so kommen neben Informationen über die Gesundheit (etwa bei Mitarbeitern mit Behinderungen) und Angaben zu einer Gewerkschaftszugehörigkeit (bei Mitgliedern des Betriebsrats) auch Daten zur religiösen Überzeugung in Betracht.[380]

Gerade bei Unternehmensakquisitionen kann es für den Interessenten äußerst wichtig sein über die Qualität des Managements und der Mitarbeiter allgemein ausreichend informiert zu sein, ist dies doch idR maßgeblich für den wirtschaftlichen Erfolg des Unternehmens und somit auch für dessen wirtschaftliche Bewertung.

---

[376] RL 95/46/EG ErwG 24.
[377] VfGH 28.11.2001, Slg 13.369.
[378] Vgl dazu *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 2, die explizit (wirtschaftliche) Daten wie Umsatz, Gewinn und Beschäftigtenzahl anführen; mwN *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 28.
[379] S dazu weiterführend *Dohr/Pollirer/Weiss*, DSG[2] I (2002) Anh V/17, 409 ff.
[380] S dazu auch Kap V.E.2.

Va bei Mitarbeitern in Vorstands- oder Geschäftsführungspositionen wird der Kaufinteressent großen Wert darauf legen, bereits im Vorhinein darüber informiert zu sein, welche Personen das Management bilden, welche Ausbildungen und Qualifikationen die einzelnen Mitarbeiter haben, auf welche Art sie vergütet werden, mit welchen Fristen ihre Verträge kündbar sind und ob Wettbewerbsverbote oder individuelle Sondervereinbarungen (bei Umstrukturierungen insb bedeutsam sind sog „Change of Control – Klauseln“[381] in Arbeitsverträgen) bestehen.[382]

3. Kundendaten

Eine weitere datenschutzrechtlich beachtliche Gruppe stellen die personenbezogenen Daten unternehmensfremder Personen dar. Als solche kommen insb die Kunden des Unternehmens in Betracht.[383]

Neben allgemeinen Kategorien wie Daten betreffend Name, Titel, Adresse etc, ist idZ ebenso an Daten über ein bestimmtes Konsumverhalten wie auch an Daten zum Zahlungsverhalten (Bonität) zu denken. All diese Informationen sind nicht zuletzt deshalb von wirtschaftlicher Werthaftigkeit, weil sie sich nicht nur zur Bindung der bereits bestehenden Kunden sondern auch zur Akquirierung neuer eignen.

Aus datenschutzrechtlicher Sicht höchst bedenklich tritt weiters der Umstand hinzu, dass sich aufgrund jüngerer Entwicklungen (auch abseits gesellschaftsrechtlicher Umstrukturierungen) der Handel mit personenbezogenen Daten von Kunden mittlerweile generell zu einem (unerlaubten) alltäglichen Geschäft entwickelt zu haben scheint.[384]

---

[381] Dabei handelt es sich um eine Regelung in Arbeitsverträgen von Vorstands- oder Geschäftsführungsmitgliedern, die diesen im Falle eines Eigentümerwechsels die Möglichkeit bietet, gegen Zahlung einer fest vereinbarten Abfindungssumme (mitumfasst ist meist auch eine entsprechende Pensionsregelung - wobei diesbezügliche Zusagen eine erhebliche finanzielle Belastung in der Zukunft bedeuten können) durch eigenen Entschluss das Unternehmen zu verlassen.

[382] *Braun/Wybitul*, Übermittlung von Arbeitnehmerdaten bei Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 785; vgl dazu auch *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 39.

[383] *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 104.

[384] Vgl dazu bspw *Bünder*, Neue Datenpanne bei der Telekom, Frankfurter Allgemeine Zeitung vom 26.11.2008; *Biermann*, Kundendaten von Monster.com geplündert, Zeit Online, 28.1.2009

D. Die Weitergabe personenbezogener Daten im Zuge der Umstrukturierung

1. Problemaufriss

Als zentraler Punkt des gegenständlichen Problems stellt sich die Frage dar, ob und bejahendenfalls welchen Tatbestand des DSG die Umstrukturierung eines Unternehmens erfüllt. Wie gezeigt wurde, ist insb die Gesamtrechtsnachfolge ein wesentliches Merkmal von Verschmelzung und Spaltung.[385] Daraus kann zwar viel über die strukturelle und organisatorische Wirkung der Umstrukturierung gewonnen werden, bezüglich der Konsequenzen für die Verwendung personenbezogener Daten dabei lässt sich jedoch prima facie nichts näheres erkennen.[386] MaW bedeutet dies, dass sich aus dem Institut der Gesamtrechtsnachfolge allein noch keine datenschutzrechtliche Aussage entnehmen lässt.

Ob die Umstrukturierung eine Verwendung von personenbezogenen Daten verwirklicht oder nicht, ist von elementarer Bedeutung für die Relevanz der datenschutzrechtlichen Diskussion dieser Vorgänge als solcher. Dass iE schließlich zahlreiche Argumente für eine datenschutzrechtliche Beachtlichkeit sprechen wird im folgenden Kap zu zeigen sein.

2. Umstrukturierungen als datenschutzrechtlich relevante Vorgänge

Versucht man Umstrukturierungsmaßnahmen einem datenschutzrechtlichen Tatbestand zu subsumieren, stellt sich vorerst jener der „Übermittlung“ iSd § 4 Z 12 DSG am aussichtsreichsten dar. Darunter ist leg cit „die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers“, zu verstehen.

Ob bei gesellschaftsrechtlichen Umstrukturierungen eine derartige Übermittlung (va im Rahmen der dabei üblichen Due Diligence Prüfungen) überhaupt stattfindet, ist jedoch

---

[385] Kap V.B.
[386] Vgl *Simitis*, Umwandlungen: ein blinder Fleck im Datenschutz?, ZHR 2001, 165.

str. Wie bereits oa ist eine Klärung dieser Frage insb deshalb von eminenter Bedeutung, da hiervon die datenschutzrechtliche Relevanz derartiger Vorgänge als solches abhängt.

Um das Nichtvorliegen einer datenschutzrechtlichen Relevanz von Umstrukturierungsmaßnahmen zu argumentieren, stützen sich die Vertreter dieser Ansicht zum einen auf das Wesen der Gesamtrechtsnachfolge als solcher, zum anderen auf die Möglichkeit einer Zuordnung personenbezogener Daten zum Vermögen der Zielgesellschaft. Diese beiden Angelpunkte der abl Lit werden nun in Folge untersucht.

a) Datenschutzrechtliche Interpretation der Gesamtrechtsnachfolge

Grundlage der abl Meinung ist die Ansicht, dass der Umstand einer Gesamtrechtsnachfolge per se das Vorliegen einer Übermittlung ausschließe.[387] Vorerst sei es keinesfalls sicher, dass eine übernehmende Gesellschaft als Vertragspartner und Rechtsnachfolger bei der Umstrukturierung überhaupt als „Dritter“ iSd datenschutzrechtlichen Diktion zu verstehen ist.

Da sich die nach dem in D geltenden § 3 Abs 7 und 8 dBDSG definierten Begriffe wie „verantwortliche Stelle“ und „Dritter“ mit den Begriffen „Auftraggeber“ und „Dritter“ nach dem österr DSG inhaltlich decken, stellt sich eine prinzipielle Übernahme der rechtswissenschaftlichen Schlüsse in das österr Datenschutzrecht iE als unproblematisch dar. Im relevanten Begriffskern ebenso kongruent stellt sich auch die „Übermittlung“ im d und österr Datenschutzrecht dar. [388]

Lüttge stützt sich vorerst auf die im dBDSG gebrauchte Formulierung des „Bekanntgebens“, dieses stellt sich nach der d Rechtslage als wesentliches Tatbestandselemet einer Übermittlung[389] dar, und versucht in weiterer Folge zu zeigen, dass ein solches bei der Universalsukzession gar nicht vorläge (dazu gleich mehr).

---

[387] *Lüttge*, Unternehmensumwandlungen und Datenschutz, NJW 2000, 2463; *Marsch-Barner/Mackenthun*, Das Schicksal gespeicherter Daten bei Verschmelzung und Spaltung von Unternehmen, ZHR 2001, 165; *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion – (k)ein Thema?, NJW 2002, 1539.

[388] Vgl dazu *Gola/Schomerus*, dBDSG[9](2007) § 3 Rz 32 und *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 13.

[389] S § 3 Z 3 dBDSG und § 4 Z 12 DSG.

Zunächst wird das Rechtsinstitut der Gesamtrechtsnachfolge näher untersucht: Diese ermögliche den Übergang von Vermögensinbegriffen ohne Anwendung des sachenrechtlichen Bestimmtheitsgrundsatzes. Dabei seien vom Wechsel der Zuordnung sämtliche aktiven und passiven Vermögensgegenstände erfasst, ohne dass es spezieller Übereignungen bzw. Übernahmen bedürfe. Die gesonderte Übergabe und Übereignung körperlicher Gegenstände sei dabei nicht erforderlich, Rechte müssten nicht abgetreten, Verbindlichkeiten nicht übernommen werden.

Diesen Schlussfolgerungen ist vorerst freilich zu folgen, zumal sich das Wesen der Gesamtrechtsnachfolge bei gesellschaftsrechtlichen Umstrukturierungen im österr und im d Recht unzweifelhaft ident darstellt.[390] Mit Eintragung der Umstrukturierung im Firmenbuch (bzw für D im Register) kommt es somit zu einem umfassenden Vermögensübergang.[391]

Voraussetzung für eine solche Durchbrechung des Spezialitätsprinzips ist dabei stets eine entsprechende gesetzliche Anordnung, wie sie sich bspw bei der Erbfolge oder eben auch bei den Vorschriften zur Umwandlung findet. Infolge der ausdrücklichen Anordnung im dUmwG könne ein Vermögensübergang im Zuge einer Gesamtrechtsnachfolge daher per definitionem nicht als das Ergebnis faktischer Transferhandlungen gesehen werden. Der Vermögensübergang sei daher sowohl bei der totalen als auch bei der partiellen Gesamtrechtsnachfolge stets nur ein rechtliches Konstrukt.[392]

Daraus folge weiters, dass bei der Gesamtrechtsnachfolge das durch faktisches Handeln gekennzeichnete Tatbestandsmerkmal des „Bekanntgebens“ iSd § 3 Abs 4 Z 3 dBDSG (und damit eine Übermittlung) nicht verwirklicht werde.[393] Die Rechtsakte einer Verschmelzung oder Spaltung seien in ihrer Tatbestandsmäßigkeit daher nicht unter das dBDSG subsumierbar, so dass iE auch keine datenschutzrechtliche Relevanz des Umstrukturierungsvorgangs gegeben sei.[394]

---

[390] *Doralt/Nowotny/Kalss*, Aktiengesetz (2003) § 219 Rz 6; *Beisel/Klumpp*, Unternehmenskauf[5] (2006) 6. Kap Rz 32.
[391] *Doralt/Nowotny/Kalss*, Aktiengesetz (2003) § 225a Rz 8; § 14 Abs 2 Z 1 SpaltG; § 2 Abs 2 Z 1 UmwG; *Kübler* in *Semler/Stengel* (Hrsg), Kurzkommentar zum dUmwG[2] (2007) § 20 Rz 8.
[392] *Lüttge*, Unternehmensumwandlungen und Datenschutz, NJW 2000, 2465.
[393] IglS *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion – (k)ein Thema?, NJW 2002, 1540.
[394] *Lüttge*, Unternehmensumwandlungen und Datenschutz, NJW 2000, 2465.

Unter Berücksichtigung der bei derartigen Umstrukturierungen regelmäßig (teilweise sogar zwingend)[395] erfolgenden Due Diligence Prüfungen kann dieser Schlussfolgerung meiner Auffassung nach jedoch nicht gefolgt werden.[396]

Bezeichnend für die Argumentation *Lüttges* ist va die Konzentration auf einen Zeitpunkt nach bereits vollzogener Umstrukturierung und der sohin bereits erfolgten Gesamtrechtsnachfolge. Letztere solle insb (mangels Vorliegen einer Übermittlung iSd § 4 Z 12 DSG) die datenschutzrechtliche Unbeachtlichkeit derartiger Vorgänge per se bewirken. Eine Behauptung, die nach dem derzeitigen Stand der Diskussion jedenfalls str scheint. Im Rahmen gesellschaftsrechtlicher Umstrukturierungen (und zwar insb bei Due Diligence Prüfungen) ist vielmehr davon auszugehen, dass es in einer überwältigenden Mehrheit der Fälle stets zu einer faktischen Übermittlung und Offenlegung personenbezogener Daten kommt.[397]

Zudem lässt sich der datenschutzrechtliche Spezialbegriff der „Übermittlung“ schon a priori nun sehr schwer mit der Konzeption und (zivilrechtlichen) Zielsetzung der Gesamtrechtsnachfolge in Einklang bringen.

Der Übermittlungstatbestand verlangt überhaupt keinen Wechsel des Eigentums, sondern stellt sich vielmehr als von der zivilrechtlichen Rechtslage losgelöst dar. Personenbezogene Daten können dabei sowohl durch Übergabe (iS eines bloßen Besitzwechsels) an körperlichen Datenträgern „übermittelt“ werden, als auch im Wege eines gänzlich unkörperlichen „Weitersagens“, das sich überhaupt als zivilrechtlich nicht einordbar darstellt.[398] Zu derartigen schlichten „Weitergaben“ von Daten wird es im Zuge des regen Informationsaustausches in den unterschiedlichen Phasen der Akquisition wohl mannigfach kommen.

Somit ist neben grds dogmatischen Überlegungen die isolierte Betrachtung des Instituts der Gesamtrechtsnachfolge vor allem im Lichte der wirtschaftlichen Praxis meiner Auffassung nach iE nicht sachgerecht.

---

[395] Bei einer geplanten Akquisition mag dies bspw die unternehmerische Vorsicht im Hinblick auf einen gesellschaftsrechtlichen Sorgfaltsmaßstab gebieten.
[396] S dazu Kap V.D.2.c).
[397] IdS auch *Wächter*, Datenschutz im Unternehmen (2003) 313 Rz 711.
[398] *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 53.

Unabhängig von Überlegungen zur Gesamtrechtsnachfolge liegt eine zu beantwortende Kernfrage jedoch va beim Umfang des zugrunde gelegten Vermögensbegriffes. Um personenbezogene Daten vor dem Hintergrund gesellschaftsrechtlicher Umstrukturierungen als von der Gesamtrechtsnachfolge erfasst interpretieren zu können, müssen sich diese va dem Vermögen des Zielunternehmens zuordnen lassen.

b) Personenbezogene Daten als von der Gesamtrechtsnachfolge umfasstes Vermögen?

Der dies für Österreich vertretenden Meinung von *Appl*[399] (die der *Lüttges* iwS entspricht) zufolge, soll eine solche Zuordnung der dem Betroffenen zustehenden Rechte an seinen personenbezogenen Daten zu einem zessionsfähigen Vermögen durchaus möglich sein. Dies wird insofern erreicht als die einzelnen, aus dem Grundrecht erfließenden Rechte mit einer wirtschaftlichen Werthaltigkeit quasi „aufgeladen" werden um iE zu einer Qualifikation als Vermögensrecht zu kommen.[400]

Dabei wird dem Betroffenen zwar durchaus ein gesetzlicher Zustimmungsvorbehalt sowie ein Widerrufsrecht hinsichtlich der Verarbeitung zugestanden, die prinzipielle Stoßrichtung dieser Argumentation geht mE dennoch fehl.

Dies, da man, wenn man dieser Ansicht konsequent folgte, iE nämlich zu einer Umdeutung des Rechts auf informationelle Selbstbestimmung zu einem bloßen Herrschaftsrecht über personenbezogene Daten bzw einem eigentumsähnlichen Ausschluss- und Verfügungsrecht käme; eine Interpretation die mit der fundamentalen Konzeption des Grundrechts auf Datenschutz meiner Auffassung nach offenkundig unvereinbar ist.[401]

---

[399] *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 98.

[400] So soll sich insb durch die Einräumung von Rechte an seinen personenbezogenen Daten durch den Betroffenen an andere eine „indirekte Werthaltigkeit personenbezogener Informationen" ergeben.

[401] IdS auch *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2007) 53.

Prinzipiell ist festzuhalten, dass sich ein Grundrecht schon kraft seiner Natur nicht zedieren lässt.[402] Zwar sind die Rechte an personenbezogenen Daten zugegebenermaßen idR eng mit dem Übergang zivilrechtlicher Rechte und Rechtsverhältnisse verbunden, daraus folgt mE jedoch nur um so mehr das Erfordernis einer den unterschiedlichen Ansätzen des Datenschutz- und allgemeinen Zivilrechts Rechnung tragenden differenzierten Untersuchung. [403]

Der Telos zivilrechtlicher Zessionsvorschriften liegt dabei unbestritten in der Übertragung des Eigentums[404] an Rechten; (gewollte) Konsequenz ist dabei, dass der Veräußerer (Zedent) das Recht nun nicht mehr innehat, während es dem Erwerber (Zessionar) fortan ausschließlich zukommt.

Dagegen räumen verfassungsgesetzlich gewährleistete Rechte ihren Trägern gerade unabhängig von rechtsgeschäftlichen Erwägungen Ansprüche ein: Auf ein solches Recht kann sich der Einzelne daher stets berufen, da es ihm de facto „permanent" aus der entsprechenden Bestimmung im Verfassungsrang erfließt. Auch für den Empfänger wären die ihm übertragenen Rechte praktisch wertlos, da diese sofort wieder im Rahmen der unmittelbaren Drittwirkung[405] bestritten werden könnten.

Zessionsfähig sind in erster Linie obligatorische Rechte: Zwar können seitens des Betroffenen durchaus anderen Personen einzelne, aus dem Grundrecht abgeleitete Rechte an seinen personenbezogenen Daten eingeräumt werden (so bspw in den Fällen der durch Zustimmung des Betroffenen gerechtfertigten Datenverwendungen), iS einer „Generalvollmacht zur Datenverarbeitung" darf dies mE jedoch keinesfalls verstanden werden.

Hinzuweisen ist dabei insb auf das Grundprinzip der informationellen Selbstbestimmung, deren Konzeption an sich gegen die Möglichkeit spricht, sich seiner

---

[402] *Neumayr* in *Koziol/Bydlinski/Bollenberger*, ABGB[2] (2007) § 1393 Rz 1; so bezieht sich auch *Appl* auf diesen Nachw der mE jedoch zutr nur iS eines Ausschlusses höchstpersönlicher Rechte von der Zession verstanden werden kann.

[403] IglS *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 38.

[404] Wenngleich die Regeln des ABGB über das Eigentumsrecht auf Rechte als unkörperliche Sachen nicht voll anwendbar sind (vgl §§ 1392 ABGB ff) wird zur Anschaulichkeit der grds verschiedenen dogmatischen Zugänge idZ die Formulierung „Eigentum" weiter gebraucht; insofern ist darunter somit stets „Eigentum iwS" zu verstehen; vgl dazu *Koziol/Welser*, Bürgerliches Recht I[13] (2006) 292.

[405] Die im österr Recht einmalig durch die Rechtswegeklausel des § 1 Abs 5 DSG angeordnet ist.

Geheimhaltungsansprüche auch nur teilweise zu begeben; insofern unterliegen personenbezogene Daten va nicht dem Eigentum (iwS) des jeweiligen Unternehmens.[406] Für sie besteht vielmehr eine eigene, durch die Bestimmungen des DSG näher ausgeformte Verwendungsordnung.[407] Dieser zufolge ist jede Verarbeitung personenbezogener Daten grds verboten.[408] Nicht umsonst ist eine abgestufte Zulässigkeitsprüfung erforderlich um iE zur Rechtmäßigkeit einer Datenverwendung zu kommen.[409] Schon hierin besteht ein wesentlicher Unterschied zu obligatorischen Rechten, die (im Rahmen der Zession) prinzipiell dem allgemeinen Rechtsverkehr freigegeben sind.

Nicht zuletzt die Höchstpersönlichkeit des Grundrechts spricht gegen die Anwendbarkeit zivilrechtsdogmatischer Übertragungstatbestände auf personenbezogene Daten. Als höchstpersönlich ist ein Recht insb dann anzusehen, wenn es von einem anderen gar nicht ausgeübt oder zumindest ohne Änderung des Inhaltes nicht auf einen anderen übertragen werden kann.[410] Wiederum ist auf die informationelle Selbstbestimmung zu verweisen, vor deren Hintergrund sich das Grundrecht auf Datenschutz jedenfalls als höchstpersönliches Recht darstellt.[411] Daher ist es meiner Auffassung nach auch nicht möglich für nur einzelne, aus dem Grundrecht abgeleitete Rechte die Möglichkeit einer Zession anzunehmen, da dies iE auf eine Aushöhlung der Selbstbestimmung hinauslaufen würde. [412]

Zusammenfassend können personenbezogene Daten mE daher nicht dem Vermögen des umzustrukturierenden Unternehmens zugezählt werden, womit iE auch eine Zession selbiger nicht in Betracht kommen kann.

---

[406] IdS auch *Simitis*, Umwandlungen: ein blinder Fleck im Datenschutz?, ZHR 2001, 165.
[407] Vgl *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 234; diesbezüglich iglS – jedoch grds für eine datenschutzrechtlichen Unbeachtlichkeit der Gesamtrechtsnachfolge - *Kübler* in *Semler/Stengel (Hrsg)*, Kurzkommentar zum dUmwG[2] (2007) § 20 Rz 11.
[408] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 6 Anm 2.
[409] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 7 Anm 5 und 6; Drobesch/Grosinger, Das neue österreichische Datenschutzgesetz (2000) 134; vgl dazu auch *Knyrim*, Datenschutzrecht (2003) 92 ff.
[410] *Ertl* in *Rummel*, ABGB[3] I (2003) § 1393 Rz 2.
[411] So wird gerade das Grundrecht auf Datenschutz von der hL als typisches Grundrecht betrachtet; vgl dazu *Aicher* in *Rummel*, ABGB[3] I (2000) § 16 Rz 24a; *Posch* in *Schwimann*, ABGB[3] I (2005) § 16 Rz 42.
[412] *Appl*, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungsmaßnahmen, GeS 2008, 98.

c) Faktischer Informationsaustausch im Vorfeld der Umstrukturierung

Als weiteres Argument für die datenschutzrechtliche Relevanz gesellschaftsrechtlicher Umstrukturierungen lässt sich schließlich die Vorbereitungs- und Prüfungsphase der geplanten Akquisition ins Treffen führen. Diese findet zumeist schon vor der eigentlichen Gesamtrechtsnachfolge statt und zT auch bereits vor Durchführung der eigentlichen Due Diligence.[413]

Bei den im Zuge der Umstrukturierungsmaßnahmen durchgeführten unterschiedlichen Arten von (bspw Legal/Tax-, Human Resource-, Commercial- oder Financial-) Due Diligence Prüfungen kommt es hernach zu vielfältigen Verwendungen personenbezogener Daten.[414]

Abgesehen von den weitgehend eigenständigen (und damit auch eine datenschutzrechtliche Auftraggebereigenschaft auslösenden)[415] Datenverarbeitungen durch die beigezogenen Prüfer sprechen mE Umfang und Vielfalt der Prüfungsmodalitäten für das Vorliegen einer Übermittlung iSd § 4 Z 12 DSG: Neben der Weitergabe personenbezogener Daten an das akquisitionswillige Unternehmen wird va auch die Datenverwendung für ein anderes Aufgabengebiet des geprüften Unternehmens[416] den Tatbestand der Übermittlung erfüllen.[417]

So ist davon auszugehen, dass eine Vielzahl personenbezogener Daten der Mitarbeiter des geprüften Unternehmens unter anderen Gesichtspunkten erfasst und analysiert werden als dies bspw nach dem Inhalt von (gerade im Personalbereich gängigen) Standardverarbeitungen der Fall ist. Zu denken ist hierbei etwa an individuelle Leistungsprofile im Rahmen einer Human Resource Due Diligence.[418]

---

413 *Berens/Mertes/Strauch* in *Berens/Brauner/Strauch* (Hrsg), Due Diligence bei Unternehmensakquisitionen[4] (2005) 55.

414 *Essers/Hartung*, Datenschutz bei Unternehmenstransaktionen, RDV 2002, 278; *Hofmann*, Due Diligence – Möglichkeiten und Grenzen des Managements (2006) 20; *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 13; mwN *Fleischer/Körber*, Due diligence und Gewährleistung beim Unternehmenskauf, BB 2001, 841; s Kap V.E.

415 S dazu insb Kap V.E.4.b).

416 In seiner Eigenschaft als Auftraggeber iSd § 4 Z 4 DSG.

417 *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Z 12 Anm 13; vgl dazu auch ErläutRV 1613 BlgNr 20. GP 39.

418 MwN *Aldering/Högemann* in *Berens/Brauner/Strauch* (Hrsg), Due Diligence bei Unternehmensakquisitionen[4] (2005) 524.

Die im Zuge der Due Diligence erfassten personenbezogenen Daten werden des weiteren wohl stets an den Kaufinteressenten übermittelt werden. Schließlich wird die Durchführung einer Due Diligence, ohne an die solcherart ermittelten Informationen zu gelangen für diesen offenkundig sinnlos sein.

Zusammenfassend ist meiner Auffassung nach daher stets vom Vorliegen einer datenschutzrechtlich relevanten Übermittlung auszugehen. Eine solche bedeutet jedoch auch immer einen Eingriff in das Grundrecht der Betroffenen auf Geheimhaltung ihrer personenbezogenen Daten und bedarf daher einer entsprechenden Rechtfertigung.[419]

3. Konsequenzen des Vorliegens einer Übermittlung – mögliche Rechtfertigungen des Grundrechtseingriffs

Wie gezeigt wurde, wird es bei gesellschaftsrechtlichen Umstrukturierungen in der überwiegenden Anzahl der Fälle zu einer Due Diligence und somit auch zu einer Übermittlung personenbezogener Daten kommen. Da durch die Übermittlung ein Verwenden von Daten[420] vorliegt, muss in einem nächsten Schritt geprüft werden, wie nun iE zu einer Rechtmäßigkeit dieses Verwendens gelangt werden kann.

a) Zustimmung der Betroffenen

Aus der bereits erwähnten inhaltlichen Vielfalt der Due Diligence werden idR auch spezifische Problemfälle betreffend der Rechtfertigung der Datenverwendung resultieren: Als einen der möglichen Ausschlussgründe für das Vorliegen schutzwürdiger Interessen (was iE die Zulässigkeit der Übermittlung bedeuten würde) sieht das DSG die Zustimmung des Betroffenen vor. Wie im Anschluss zu zeigen sein wird, wird eine solche Zustimmung jedoch den strengen datenschutzrechtlichen Anforderungen nur in den seltensten Fällen tatsächlich entsprechen können. Ungeachtet des Umstandes, dass die datenschutzrechtliche Zustimmung insb im privaten Bereich

[419] Die Übermittlung bedarf dabei insb in Hinblick auf den aus dem Grundrecht abgeleiteten Anspruch der Betroffenen auf Schutz vor Ermittlung und Schutz vor Weitergabe der über sie ermittelten Daten einer Rechtfertigung; s ErläutRV 1613 BlgNR 20. GP 34.
[420] § 4 Z 8 DSG.

weit verbreitet und von dementsprechender Bedeutung ist,[421] ist dieser Rechtfertigungsgrund im interessierenden Fall mE nur wenig tauglich.

Die Erfüllung der in § 4 Z 14 DSG normierten Voraussetzungen, wonach unter der leg cit „Zustimmung, die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den Fall in die Verwendung seiner Daten einwillig;“, zu verstehen ist, dürfte nämlich in Hinblick auf jene Gruppen von Betroffenen[422], für die eine Zustimmungserklärung durch die Vertretungsorgane des umzustrukturierenden Rechtsträgers nicht in Frage kommt, erhebliche Schwierigkeiten bereiten.[423]

So wird sich für den komplexen Bereich der Wirtschafts- bzw Due Diligence Prüfung eine umfassende Aufklärung über die konkrete Sachlage von bspw allen Mitarbeitern, deren personenbezogene Daten verarbeitet werden iE nicht selten als praktisch undurchführbar erweisen.

Anders wird sich mE jedoch die Situation im Hinblick auf jene personenbezogenen Daten verhalten, die das umzustrukturierende Unternehmen selbst betreffen. Da den vertretungsbefugten Organen der Zielgesellschaft im Wesentlichen bewusst sein wird, in welchem Ausmaß und zu welchem Zweck die das Unternehmen (bzw dessen Rechtsträger) betreffenden Daten verarbeitet werden, können sie auch eine datenschutzrechtlich wirksame Zustimmung erteilen. Dass eine solche gegebenenfalls nicht explizit erfolgt schadet nicht, da eine ausdrückliche Zustimmung nicht erforderlich ist. [424] Eine solche ist nach dem DSG nur für sensible Daten vorgeschrieben, diese kommen bei juristischen Personen jedoch nicht in Betracht.[425]

---

[421] Vgl dazu *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 185.
[422] Zu denken ist insb an natürliche Personen wie Mitarbeiter und Kunden des betroffenen Unternehmens im Gegensatz zu diesem Unternehmen als selbst datenschutzrechtlich Betroffenem; s Kap V.D.2. und Kap V.D.3.
[423] Vgl *Dohr/Pollirer/Weiss*, DSG^2 I (2002) § 4 Anm 15; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 125.
[424] Dohr/Pollirer/Weiss, DSG^2 I (2002) § 4 Anm 15; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 125.
[425] *Knyrim*, Datenschutzrecht (2003) 16.

b) Überwiegendes Interesse des Auftraggebers oder eines Dritten

Als weiterer in der unternehmerischen Praxis bedeutender Rechtfertigungsgrund einer Datenverarbeitung kommt schließlich das Vorliegen eines überwiegenden Interesses des Auftraggebers[426] oder eines Ditten in Betracht; wobei als Standardfall die Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem anzusehen sein wird.[427]

Fraglich ist nun erstens worin diese überwiegenden Interessen des Auftraggebers bestehen können: Nach der allgemeinen juristischen wie datenschutzrechtlichen Terminologie ist unter berechtigtem Interesse ein rechtliches oder rechtlich geschütztes Interesse nicht nur dann zu verstehen, wenn es unmittelbar normiert ist, sondern auch wenn es in der Rechtsordnung nicht ausdrücklich geschützt ist (also erst aus dem Recht bzw der Gesamtrechtsordnung abgeleitet werden muss).[428]

Dies können wirtschaftliche wie auch ideelle Interessen sein. Zu den wirtschaftlichen Interessen lassen sich idZ betriebswirtschaftliche Vorteile, wie etwa die Vermeidung oder Minimierung von Risiken, insb von Verlusten zählen.

Die Offenlegung betriebswirtschaftlicher Interna stellt sich weiters als wesentliche Entscheidungsvoraussetzung für ein übernehmendes Unternehmen dar und hat maßgebliche Bedeutung dafür, ob es in eine geplante Akquisition einwilligt oder nicht. Aus diesem Grund wird die Zurverfügungstellung personenbezogener Daten für das geprüfte Unternehmen in den meisten Fällen unausweichlich sein.

Mit *Schaffland* darf die Frage gestellt werden: „Wer fusioniert schon mit einem Rechtsträger, dessen wirtschaftliche Situation nicht bekannt ist?“.[429] Unabhängig davon

---

[426] § 8 Abs 1 Z 4 DSG; bemerkenswert idZ ist die Formulierung des Erlaubnistatbestandes in § 8 Abs 3 Z 4 DSG, der dem Recht des Betroffenen insofern einen höheren Stellenwert als Art 7 lit f der RL 95/46/EG beimisst, da nicht dieser, sondern der Auftraggeber der Datenverarbeitung ein überwiegendes Interesse an selbiger glaubhaft zu machen hat; vgl dazu auch *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 139.

[427] § 8 Abs 3 Z 4 DSG; s dazu auch *Knyrim*, Datenschutzrecht (2003) 163.

[428] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 1 Anm 13.

[429] *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion – (k)ein Thema?, NJW 2002, 1541.

ist freilich auch an solche Fälle zu denken, in denen das Zustandekommen der geplanten Umstrukturierung überwiegend im Interesse der Zielgesellschaft liegt.[430]

Auch wirtschaftliche Interessen des übernehmenden Rechtsträgers als Dritten iSd § 8 Abs 1 Z 4 DSG sind zu bedenken. Zu beachten ist freilich, dass die Interessen des Käufers mit jenen der Mitarbeiter und Kunden[431] des avisierten Unternehmens wohl seltener kongruent sein werden, als deren Interessen mit jenen des avisierten Unternehmens selbst.[432] Aus diesem Grund wird eine Interessenabwägung in einem solchen Fall mE eher zugunsten der Schutzwürdigkeit genannter Personengruppen ausfallen.[433]

Als nähere Konkretisierung der Generalklausel in § 8 Abs 1 Z 4 DSG enthält Abs 3 der Bestimmung schließlich einige der wichtigsten Fälle, in denen durch die Datenverwendung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden. Es erscheint idZ sinnvoll insb die Erfüllung vertraglicher Verpflichtungen[434] als einen der von Unternehmen am häufigsten vorgebrachten Ausnahmegründe näher zu untersuchen.

c) Die Erfüllung vertraglicher Verpflichtungen

In unmittelbarem Bezug auf die Umstrukturierungsmaßnahme wird sich aus der (meist) arbeitsvertraglichen Rechtsbeziehung zwischen den Betroffenen und dem umzustrukturierenden Unternehmen (als datenschutzrechtlichem Auftraggeber) mE jedoch nur wenig gewinnen lassen.

Dieser Rechtsfertigungstatbestand ist va deshalb grds wenig tauglich um Übermittlungen im Zuge der Due Diligence Prüfungen zu rechtfertigen, da sich der rechtliche Inhalt der diesbezüglichen Verträge typischerweise auf die zwischen dem Unternehmen und seinen Mitarbeitern, Kunden oder Lieferanten bestehenden

---

[430] So etwa im Fall der „Rettung durch Übernahme“ eines insolvenzbedrohten durch ein kapitalstarkes Unternehmen; für D vgl dazu *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 25.
[431] In ihrer Eigenschaft als datenschutzrechtlich Betroffene.
[432] IdS *Zimmermann*, Interne und externe Kommunikation in *Picot* (Hrsg) Handbuch Mergers & Acquisitions[3] (2005) 491.
[433] Vgl *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 8 Anm 9.
[434] § 8 Abs 3 Z 4 DSG.

Rechtsbeziehungen beschränken wird. Zumindest für die letztgenannten Personengruppen wird schon ihrem Wesen nach keine Vertragsbeziehung bestehen, aus der sich entsprechende Rechtfertigungen für ein bestimmtes Verhalten bei (oder im Vorfeld von) Umstrukturierungssituationen erkennen ließe. Eine Rechtfertigung der Datenverarbeitung durch die Erfüllung einer vertraglichen Verpflichtung kann diesfalls daher schon mangels Bestehen einer solchen nicht Betracht kommen.

So muss im vorliegendem Fall iE wohl auf den allgemeinen Rechtfertigungstatbestand des § 8 Abs 1 Z 4 DSG zurückgegriffen werden, wonach wiederum eine Interessenabwägung vorgenommen werden muss.[435]

Eine auf vertragliche Beziehungen gestützte Rechtfertigung kann meiner Auffassung nach jedoch für jene personenbezogenen Daten möglich sein, bei denen das umzustrukturierende Unternehmen selbst Betroffener ist. Jenes wird vor Beginn der eigentlichen Transaktion mit dem akquisitionswilligen Unternehmen zumeist Unterlagen zur Fixierung erster Eckpunkt der Umstrukturierung (einen sog „Letter of Intent“) erarbeiten, aus denen sich bereits bestimmte Informationspflichten des Zielunternehmens gegenüber dem potentiellen Käufer ergeben.[436] Auch derartige Absichtserklärungen können mE zumindest Anhaltspunkte für die Rechtmäßigkeit einer Datenverarbeitung geben.

Abgesehen davon kann im Hinblick auf den die Akquisition selbst regelnden Vertrag das Zurverfügungstellen von Informationen als Durchführung vorvertraglicher Maßnahmen in Betracht kommen.

Aus datenschutzrechtlich besonders interessierender Sicht kann hier exemplarisch auf die Abläufe einer Human Resource Due Diligence hingewiesen werden. Dort kommt es vor dem eigentlichen Abschluss oder der Wirksamkeit des Vertrages zu einem Austausch von (oft auch sensiblen) Mitarbeiterdaten. *Knyrim*[437] sieht hierin bspw vorvertragliche Maßnahmen; eine Ansicht der mE gefolgt werden kann und die ebenso auf alle anderen Formen der Due Diligence umgelegt werden kann. Wie gezeigt wurde,

---

[435] IdS auch *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 240.
[436] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 17; *Beisel/Klumpp*, Unternehmenskauf[5] (2006) 19. Kap Rz 15.
[437] *Knyrim*, Datenschutzrecht (2003) 103.

besteht jedoch der hier maßgebliche Vertrag nicht zwischen den Mitarbeitern und dem jeweiligen akquisitionswilligen Unternehmen, sondern vielmehr zwischen Kaufinteressenten und dem Zielunternehmen (als dem Arbeitgeber der betroffenen Mitarbeiter).

Dem DSG lässt sich zwar (im Gegensatz zur europarechtlichen Vorgabe)[438] keine einschlägige Regelung zur Datenverarbeitung im Zuge vorvertraglicher Maßnahmen entnehmen, doch wird diese wohl dennoch als tauglicher Rechtfertigungsgrund anzusehen sein, sofern sie der allgemeinen Interessensabwägung nach § 8 Abs 1 Z 4 DSG standhält.[439]

Da eine solche Maßnahme jedoch auf Antrag des Betroffenen erfolgen muss, scheint eine Rechtfertigung der Datenverarbeitung (ebenso wie bei der Zustimmung) meiner Auffassung nach nur für personenbezogene Daten des umzustrukturierenden Unternehmens selbst denkbar.

[438] Art 7 lit b RL 95/46/EG; vgl dazu krit *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 47.
[439] IglS *Knyrim*, Datenschutzrecht (2003) 102.

4. Grenzen der Übermittlung aus dem Gesellschaftsrecht?

Neben den datenschutzrechtlichen Bestimmungen werden bei einer Verwendung personenbezogener Daten va auch Vorgaben aus dem Gesellschaftsrecht zu beachten sein. Im Folgenden werden daher der allgemeine Informationsfluss in der Gesellschaft sowie die besondere Situation einer Umstrukturierung dargestellt.

a) Der allgemeine Informationsfluss in der Gesellschaft

Das bei Kapitalgesellschaften typische Informationsregime im Verhältnis Vorstand/Aufsichtsrat[440] ist grds mehrschichtig aufgebaut; es besteht bei näherer Betrachtung aus einem System von Bringschulden des Vorstands einerseits und Holschulden des Aufsichtsrats andererseits.

Im Verhältnis zwischen Vorstand und Aufsichtsrat ist von besonderem Interesse, welche Informationen der Vorstand seinem Aufsichtsrat übermitteln muss, damit dieser seiner gesetzlich verankerten Überwachungspflicht[441] überhaupt nachkommen kann, wie weit der Aufsichtsrat umgekehrt selbst nach bestimmten Informationen nachfragen muss, und aber auch, ob bzw unter welchen Umständen ein Recht oder sogar eine Verpflichtung des Vorstands besteht, dem Aufsichtrat bestimmte Informationen vorzuenthalten.[442]

Letzteres kann va dann der Fall sein, wenn dem Aufsichtsrat auch Vertreter eines konkurrierenden Unternehmens angehören und der Vorstand aus diesem Grund über einzelne zukunftsträchtige Projekte nicht im Detail informieren möchte bzw wenn sich Projekte in einem Planungsstadium befinden und eine vorzeitige Realisierung gefährden

---

[440] Zu den idZ nicht zu problematisierenden, jedoch grds ähnlich gelagerten, Fragestellungen im Verhältnis Aufsichtsrat – Aktionär vgl *Arnold*, Die Pflicht des Vorstandes zur Auskunftsverweigerung in der Hauptversammlung, GesRZ 2007, 99 (101).

[441] § 95 Abs 1 AktG; da in der gegenständlichen Problematik va der Informationsfluss iZm mit der dualistischen Konstruktion im österr Gesellschaftsrecht interessiert, wird der Schwerpunkt der Untersuchung auf die AG gelegt.

[442] *Kalss*, Geheimnisschutz – Datenschutz – Informationsschutz im Gesellschaftsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg) Geheimnisschutz Datenschutz Informationsschutz (2008) 249.

würde.[443] Im Hinblick auf den Datenschutz interessiert jedoch va das (Außen-) Verhältnis zwischen dem Unternehmen und dem Akquisitionsinteressenten als Drittem.

Als eine solche für die Verpflichtung zur Geheimhaltung (personenbezogener) Daten charakteristische Situation stellen sich dabei Due Diligence Prüfungen im Zuge von Umstrukturierungen dar.

b) Die Weitergabe von Informationen im Zuge der Umstrukturierung – Die Due Diligence als Anlassfall

Vorerst ist festzuhalten, dass die aktienrechtliche Schweigepflicht grds nicht absolut gelten kann. Dies wird sich schon aus dem Schutzzweck ergeben, liegt es schließlich im Interesse der Gesellschaft, wenn Vorstandsmitglieder Betriebs- und Geschäftsgeheimnisse an nachgeordnete Mitarbeiter der Gesellschaft oder externe Berater weitergeben, um sie damit überhaupt erst nutzen zu können.[444]

Da Akquisitionsinteressenten als außenstehende Dritte gegenüber dem Unternehmen keinen (gesellschaftsrechtlichen) Informationsanspruch haben, ist zu klären, ob der Vorstand von sich aus Unternehmensinterna weitergeben darf. Zu beachten ist dabei stets das „Wohl des Unernehmens“ iSd § 70 Abs 1 AktG.[445]

Gebietet es das Unternehmenswohl, die geplante Akqusition durch Einsichtgewährung in unternehmensbezogene Daten zu fördern, wird eine entsprechende Vereinbarung gerechtfertigt sein.[446] Zu beachten wird jedoch sein, dass nicht mehr an Informationen preisgegeben wird, als zum einen für die Meinungsbildung des Interessenten erforderlich und zum anderen in Anbetracht der zu beachtenden Schutzzwecke des Verschwiegenheitsgebotes zumutbar und zulässig ist.[447]

---

[443] *Sina*, Zur Berichtspflicht des Vorstandes gegenüber dem Aufsichtsrat bei drohender Verletzung der Verschwiegenheitspflicht durch einzelne Aufsichtsratmitglieder, NJW 1990, 1018.
[444] IglS *Krejci*, Verschwiegenheitspflicht des AG-Vorstands bei Due-Diligence-Prüfungen, RdW 1999, 574.
[445] Vgl *Mader*, Kapitalgesellschaften[6] (2008) 71.
[446] IdS auch *Bihr*, Due Diligence: Geschäftsführungsorgane im Spannungsfeld zwischen Gesellschafts- und Gesellschafterinteressen, BB 1999, 1201.
[447] *Krejci*, Verschwiegenheitspflicht des AG-Vorstands bei Due-Diligence-Prüfungen, RdW 1999, 575.

Auch nach gesellschaftsrechtlichen Vorschriften ist somit eine Interessensabwägung vorzunehmen: Die Herausgabe[448] von unternehmensbezogenen Daten im Rahmen einer Due Diligence wird idR immer dann als gerechtfertigt zu betrachten sein, wenn sie im Interesse (und somit im Wohl) des Unternehmens liegt. Die aus dem Gesellschafts- wie Datenschutzrecht jeweils vorzunehmenden Wertungen stellen sich daher iE als durchaus vereinbar dar.

Festzuhalten ist idZ auch, dass die gesellschaftsrechtlichen Bestimmungen zum Geheimnisschutz freilich nur für die beteiligten geschäftsführenden Organe Verbindlichkeit entfalten werden können. Bei der Weitergabe von Informationen durch die im Rahmen einer Due Diligence beigezogenen Prüfer sind für letztere (neben etwaigen berufsrechtlichen Geheimhaltungspflichten)[449] die entsprechenden Bestimmungen des DSG maßgeblich.[450]

[448] Die nach datenschutzrechtlicher Diktion einer Übermittlung iSd § 4 Z 12 DSG entspricht.
[449] Vgl dazu bspw § 91 WTBG.
[450] S dazu Kap V.E.6.

E. Die Due Diligence Prüfung

Im folgenden Kap wird nun ein Überblick über das Wesen und den datenschutzrechtlichen Gehalt der bei gesellschaftsrechtlichen Umstrukturierungen typischerweise stattfindenden Due Diligence Prüfungen gegeben.

1. Herkunft und Bedeutung

Wie bereits dargelegt[451], ist es bei Käufen von ganzen Unternehmen, größeren Aktienpaketen oder anderen Gesellschaftsbeteiligungen mittlerweile weit geübte Praxis, dass der Kaufinteressent vor Abschluss eines bindenden Vertrages Einsicht in das Unternehmen durch Sachverständige verlangt. Damit soll va das Risiko des Käufers hinsichtlich seiner Annahmen bei der Unternehmensbewertung reduziert werden.

Die Wurzeln des Begriffs „Due Diligence" liegen jedoch weniger in der Praxis der Unternehmens- und Beteiligungskäufe als vielmehr im US-amerikanischen Bundeskapitalmarkt- und Anlegerrecht.[452] Hierbei wird jener Sorgfaltsmaßstab als „due diligence" bezeichnet, den der Emittent von Wertpapieren sowie die ihn unterstützenden Sachverständigen bei der Erstellung des Prospekts für einen Börsegang einzuhalten haben.[453]

Wurde mit der Formulierung „due diligence" zu Beginn lediglich ein Sorgfaltsmaßstab bezeichnet, fand der Begriff später auch im Bereich des Unternehmenskaufes Verwendung. Dazu wesentlich beigetragen hat insb das im angloamerikanischen Rechtskreis geltende Rechtsprinzip „caveat emptor", wonach den Verkäufer einer Sache nur sehr eingeschränkte Informationspflichten treffen.[454]

Demzufolge hat der Käufer das Risiko für etwaige Mängel zu tragen und ist daher naturgemäß bestrebt auf die Ausarbeitung eines eigenen vertraglichen

---

[451] Vgl dazu schon die ganz grds Ausführungen im Vorwort.
[452] *Berens/Strauch* in *Berens/Brauner/Strauch* (Hrsg), Due Diligence bei Unternehmensakquisitionen[4] (2005) 6.
[453] Dieses Verfahrens trat erstmals formalisiert im „US Securities Act of 1933" in Erscheinung; zum genauen Wortlaut der Bestimmung s die Homepage der US Securities and Exchange Comission, abrufbar unter http://uscode.house.gov/download/pls/15C2A.txt (11.12.2008).
[454] MwN *Merkt*, Due Diligence und Unternehmenskauf, BB 1995, 1041

Gewährleistungsregimes hinzuwirken, wenn der Verkäufer für bestimmte Eigenschaften des Kaufobjekts einstehen soll.
Dem voraus geht wiederum eine eingehende Überprüfung des Kaufgegenstandes, für die als Bezeichnung schließlich Due Diligence gebräuchlich wurde.

2. Mögliche Inhalte einer Due Diligence Prüfung

Einen stets gleichbleibenden Inhalt für eine Due Diligence anzugeben ist aufgrund der variierenden Prüfungsinteressen nicht möglich. Je nach Informationsbedürfnis des Käufers werden sich die Schwerpunkte einer Unternehmensprüfung verschieden darstellen, so wird ein Unternehmen der Technologiebranche den Erfolg oder Misserfolg einer Akquisition (bzw Umstrukturierung) von anderen Faktoren abhängig machen als etwa ein Leiharbeitsunternehmen.[455]

Bei einer wirtschaftlichen Due Diligence (Commercial Due Diligence) werden das wirtschaftliche Umfeld, die Marktposition der Zielgesellschaft, ihre Produktion sowie Vertriebswege und Organisationsstruktur untersucht.[456] Da diese Form der Due Diligence va profunde Kenntnisse in der Branche der Zielgesellschaft voraussetzt werden oftmals Unternehmensberater oder auch Investmentbanken beigezogen.[457]

Bei der finanziellen Due Diligence (Financial Due Diligence) findet eine genaue Analyse der Jahresabschlüsse des Unternehmens statt. Zu diesem Zweck überprüfen Wirtschaftsprüfer Unterlagen des Controlling und Rechnungswesens sowie Verkaufsstatistiken und andere diesbezüglich relevante Unternehmensinterna.[458]

Um Risiken aus rechtlichen Belangen zu vermeiden wird eine rechtliche und steuerliche Due Diligence (Legal bzw Tax Due Diligence) durchgeführt. Bei ersterer werden der rechtliche Rahmenbereich der Zielgesellschaft sowie alle Aspekte, die für eine ordnungsgemäße Abwicklung von Transaktionen und die Vertragsgestaltung erforderlich sind, bei letzterer alle steuerlichen Gesichtspunkte (wie bspw

[455] Vgl *Hofmann*, Due Diligence – Möglichkeiten und Grenzen des Managements (2006) 20.
[456] *Fleischer/Körber*, Due diligence und Gewährleistung beim Unternehmenskauf, BB 2001, 841.
[457] *Krüger/Kalbfleisch*, Due Diligence bei Kauf und Verkauf von Unternehmen – rechtliche und steuerliche Aspekte der Vorprüfung beim Unternehmenskauf, DStR 1999, 175.
[458] Vgl *Spill*, Due Diligence – Praxishinweis zur Planung, Durchführung und Berichterstattung, DStR 1999, 1787.

Steuerhaftungsrisiken und steueroptimale Strukturierung), auf die bei der geplanten Unternehmensumstrukturierung Bedacht zu nehmen ist, untersucht.[459]

Eine weitere, insb datenschutzrechtlich interessierende, Form der Due Diligence stellt die sog Human Resource Due Diligence dar.[460] Gegenstand der Untersuchung sind hierbei va arbeitsrechtliche Belange: Neben einer Übersicht über die einzelnen Mitarbeiter sowie einer Kurzbeschreibung mit Funktion, (Dienst-) Alter, Entgeltsansprüchen und Kündigungsfristen kommen auch eine Darstellung über die kollektiven Mitarbeitervertretungsorgane und deren Mitglieder sowie anzuwendende Betriebs- und Kollektivvereinbarungen in Betracht.[461]

Datenschutzrechtlich stellt sich die Human Resource Due Diligence weiters auch insofern problematisch dar, als hierbei typischerweise auch sensible Daten iSd § 4 Z 2 DSG verarbeitet werden. So sind bspw Angaben über Mitarbeiter mit Behinderungen[462], Informationen zum Religionsbekenntnis[463] sowie die Zugehörigkeit zu einer Gewerkschaft oftmals von vitalem Interesse für das Unternehmen und solcherart entsprechend dokumentiert.[464]

3. Funktionen und beteiligte Interessen bei der Due Diligence Prüfung

Der Hauptzweck einer im Rahmen einer Unternehmensumstrukturierung durchgeführten Due Diligence liegt in der Ermöglichung einer tunlichst genauen Abwägung von Risiko und Kosten für einen potentiellen Vertragspartner bzw eine übernehmende Gesellschaft.[465]

Bei derartigen Umstrukturierungen hat der Verkäufer typischerweise einen erheblichen Informations- und Wissensvorsprung gegenüber dem Käufer, insb was die für das Unternehmen wichtigen Kennzahlen (wie bspw Bilanzen und Jahresabschlüsse) betrifft. Das zu akquirierende Unternehmen wird weiters naturgemäß bestrebt sein, die von ihm

---

[459] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 13.
[460] *Gran*, Abläufe bei Mergers und Acquisitions, NJW 2008, 1413.
[461] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 38.
[462] So bspw das Bestehen eines besonderen gesetzlichen Kündigungsschutzes.
[463] Dies va im Hinblick auf die jeweiligen gesetzlichen Feiertage.
[464] Vgl dazu *Braun/Wybitul*, Übermittlung von Arbeitnehmerdaten bei Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 785.
[465] *Gran*, Abläufe bei Mergers und Acquisitions, NJW 2008, 1410.

dem Käufer vorgelegten Zahlen und zu erwartende Erträge, Umsätze, Gewinn- und Verlustrechnungen entsprechend positiv darzustellen.

Generell ist festzuhalten, dass die Begründung von Geschäftsbeziehungen und der Abschluss von Verträgen durch unvollkommene Informationen gekennzeichnet sind, da wohl stets eine Seite gegenüber der anderen Seite einen gewissen Informationsvorsprung besitzen wird. Bei gesellschaftsrechtlichen Umstrukturierungen wie einem Unternehmenskauf ist der potentielle Käufer daher gehalten, diesen Zustand unvollkommener Informationen durch entsprechende Informationsaktivitäten zu beseitigen.[466]

Neben dem Aufdecken von Risiken wie bspw schadhaften Produktionsanlagen, fehlenden Betriebsanlagengenehmigungen oder Steuerschulden kann der Akquisitionsinteressent durch die Due Diligence va auch die von ihm erhofften Chancen verifizieren.

So ist dieser bei Übernahme einer erheblichen Beteiligung[467] oftmals bestrebt, hierdurch Synergieeffekte oder Know-how für bereits bestehende Unternehmen in seinem Eigentum zu gewinnen. Ob sich die strategischen Absichten des Käufers durch eine avisierte Umstrukturierung tatsächlich verwirklichen lassen, kann zumeist erst nach Einsicht in die Zielgesellschaft beurteilt werden. Wie bereits dargelegt wird die Durchführung einer Due Diligence somit va auf die Überprüfung der mit der Akqusition erhofften Chancen gerichtet sein.[468]

Auf Verkäuferseite ist auch zu erwähnen, dass dieser durch die Due Diligence nicht zuletzt auch in die Lage versetzt wird sein eigenes Risiko, nämlich einen potentiell zu niedrigen Kaufpreis zu erhalten, dadurch minimieren kann, als etwaige rechtzeitig erkannte Probleme schon im Vorfeld (also schon vor Erteilung der ersten Informationen an die Käuferseite) behoben werden können.

---

[466] *Beisel/Klumpp*, Unternehmenskauf[5] (2006) 2. Kap Rz 1.
[467] Sog Share-Deal; s auch *Rauter*, Unternehmenserwerb, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) 318.
[468] Vgl *Hofmann*, Due Diligence – Möglichkeiten und Grenzen des Managements (2006) 25.

Zu diesem Zweck kann eine Unterstützung durch externe Berater dem Verkäufer zu einer effizienteren Due Diligence Vorbereitung mit aktiver Problembehebung verhelfen und damit seine Verhandlungsposition entscheidend stärken.[469]

Mit *Fleischer/Körber* lassen sich zusammenfassend im Wesentlichen folgende Funktionen einer Due Diligence für den Käufer festhalten:[470]

1. Gewährleistungsfunktion (diese wird erreicht durch eine eingehende Prüfung des Zustandes der Zielgesellschaft bzw durch entsprechende Absicherung mittels vertraglicher Gewährleistungen und Garantien[471])
2. Risikoermittlungsfunktion (Informationsbeschaffung- und Verifizierung, ob das Unternehmen den Erwartungen des Käufers entspricht und ob aus dem Verkauf besondere Risiken herrühren)
3. Wertermittlungsfunktion (so haben die im Rahmen der Due Diligence gewonnenen Erkenntnisse unmittelbaren Einfluss auf die Höhe des Kaufpreises[472])
4. Beweissicherungsfunktion (Feststellung des Istzustandes eines Unternehmens sowie Dokumentation des Informationsflusses zwischen Zielgesellschaft/Verkäufer und Käufer)

Nach durchgeführter Due Diligence steht der Kaufinteressent idR vor einer Vielzahl (personenbezogener) Informationen über die Zielgesellschaft und hat somit sein ursprünglich bestehendes Informationsdefizit beseitigt. Solcherart ist er nun in der Lage eine abschließende Entscheidung zu treffen, ob und unter welchen Bedingungen er die geplante Akqusition vornehmen will.

---

[469] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 18.
[470] *Fleischer/Körber*, Due diligence und Gewährleistung beim Unternehmenskauf, BB 2001, 842; auf diese Aufzählung Bezug nehmend *Beisel/Klumpp*, Unternehmenskauf[5] (2006) 2. Kap Rz 4.
[471] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 29.
[472] IdS *Kiethe*, Vorstandshaftung aufgrund fehlerhafter Due Diligence beim Unternehmenskauf, NZG 1999, 977.

4. Die datenschutzrechtlichen Akteure der Due Diligence Prüfung

Bevor auf den datenschutzrechtlichen Gehalt der im Zuge der Due Diligence auftretenden Personen und vorgenommen Handlungen einzugehen ist, wird idZ nochmals ein kurzer Überblick über die im Datenschutzrecht typischerweise gegebene Trias von Auftraggeber, Betroffenem und Dienstleister gegeben.[473]

Der Auftraggeber ist stets „Herr der Daten", er ist – ohne Rücksicht auf den Umfang seiner eigenen Mitwirkung bei der Datenanwendung – allein dafür verantwortlich, dass eine Verwendung personenbezogener Daten nur in gesetzeskonformer Art und Weise erfolgt. Er ist außerdem primärer Ansprechpartner für sämtliche Beteiligten (anhand der DVR-Nr lässt sich der Auftraggeber zumeist problemlos über das DVR eruieren).[474] Der Auftraggeber besitzt weiters gegenüber dem Betroffenen Ansprüche auf Kostenersatz für die Erteilung von Auskünften[475] sowie auf Löschung des Bestreitungsvermerkes.[476]

Dem Betroffenen steht das Grundrecht auf Geheimhaltung seiner personenbezogenen Daten zu. Zur näheren inhaltlichen Ausgestaltung dieses Rechtes wird auf die diesbezüglichen Ausführungen in Kap IV.A.I. verwiesen.

Den Dienstleister treffen schließlich gesetzliche (und gegebenenfalls auch vertragliche) Pflichten gegenüber dem Auftraggeber oder einem allfälligen Sub-Dienstleister. Dafür stehen diesem jedoch auch Rechte gegenüber dem Auftraggeber der Datenverarbeitung zu wie bspw der Anspruch auf den vereinbarten oder angemessenen Werklohn. Ist ein Sub-Dienstleister vorhanden, besteht für den Dienstleister gegen diesen insb der Anspruch auf die vertragskonforme Erfüllung des Sub-Auftrages.[477]

Im Anschluss werden nun die im Rahmen der Due Diligence typischerweise beteiligten Personen nach ihrer Rolle im datenschutzrechtlichen Regime untersucht.

---

[473] Zu den Legaldefinitionen des § 4 DSG s FN 312, 313 und 314.
[474] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) XXVI.
[475] § 26 Abs 6 DSG.
[476] § 27 Abs 7 letzter Satz DSG.
[477] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) XXVXXVIII.

a) Der Verkäufer

Die Frage welche Rolle der zu verkaufende bzw umzustrukturierende Rechtsträger hat ist in der Lit nicht eindeutig beantwortet.

Eine Ansicht vertritt die Auffassung, dass die Due Diligence va vom Akquisitionsinteressenten als Prüfenden verlangt wird, wonach man vorerst zum Ergebnis käme, dass derjenige, der die Prüfung durchführt als datenschutzrechtlicher Auftraggeber zu betrachten ist.[478]

Die Vertreter dieser Meinung führen in weiterer Folge jedoch selbst aus, dass eine solche Qualifikation des Prüfenden iE absurde Rechtsfolgen zeitigen würde: Den Prüfenden träfen somit nämlich die datenschutzrechtlichen Vorgaben und Pflichten in Bezug auf die Einhaltung schutzwürdiger Geheimhaltungsinteressen[479], die Datensicherheit[480], die Informationspflicht[481], die Offenlegungspflicht[482] und die Richtigstellung und Löschung von Daten[483].

Daher müsse die Ableitung aus der Definition des Auftraggebers entsprechend angepasst werden: Dies gelinge va durch den Umstand, dass es stets der Geprüfte ist, der eine Einwilligung in die Durchführung der Due Diligence erteilt und somit eine „Entscheidung" iSd der Definition des § 4 Z 4 DSG trifft.
IE sei daher der Geprüfte, dh das Unternehmen selbst, als datenschutzrechtlicher Auftraggeber zu qualifizieren, der somit auch die diesem obliegenden Pflichten entsprechend zu erfüllen habe.

Dieser Auffassung wird von der abl Meinung entgegengehalten, dass es vielmehr der Eigentümer des Unternehmens sei, der als Auftrageber auftritt. Dieser träfe als

---

[478] *Feltl/Mosing*, Das Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 238.
[479] §§ 8 und 9 DSG.
[480] § 14 DSG.
[481] § 24 DSG.
[482] § 25 DSG.
[483] § 27 DSG.

Veräußerer im Rahmen der Due Diligence[484] die Entscheidung, welche Daten in welcher Form zur Verfügung gestellt werden.[485]

Dieser Ansicht ist meiner Auffassung nach jedenfalls zu folgen, zumal sie sich bereits aus dem Wortlaut der Definition des datenschutzrechtlichen Auftraggeberbegriffes ergibt: Auftraggeber ist derjenige, der die Entscheidung getroffen hat Daten für einen bestimmten Fall zu verarbeiten. Im gegenständlichen Fall also die Entscheidung, dass zwecks Ermöglichung der Akquisition eine Due Diligence Prüfung durchzuführen ist in deren Rahmen personenbezogene Daten verarbeitet werden.

Maßgeblich für die Qualifikation als Auftraggeber ist der faktische Umstand der alleinigen Entscheidung zur Datenverarbeitung.[486] Das Recht das Unternehmen zu verkaufen bzw umzustrukturieren ist unzweifelhaft dem daran dinglich vollberechtigten[487] und somit dem Eigentümer vorbehalten; nur diesem allein kann mE daher die Entscheidungsbefugnis und somit Auftraggebereigenschaft zukommen.

Zusammenfassend ist daher festzuhalten, dass bezüglich der Verwendung personenbezogener Daten im Zuge eines Unternehmenskaufes (zumindest in der ersten Phase)[488] stets der Eigentümer des Unternehmens als datenschutzrechtlicher Auftraggeber iSd § 4 Z 4 DSG zu betrachten ist.

b) Die Prüfer der Due Diligence

Der Umstand, dass bei gesellschaftsrechtlichen Umstrukturierungen mittlerweile nahezu ausnahmslos entsprechend versierte Sachverständige zugezogen werden lässt sich auf mehrere Gründe zurückführen: Zum einen auf die diesbezüglichen europarechtlichen Vorgaben, nämlich Art 10 RL 78/855/EWG[489] bzw Art 8 RL 82/891/EWG[490], die bei

---

[484] Unzweifelhaft kommt dem Veräußerer somit auch die Entscheidung zu, ob überhaupt eine Due Diligence stattfindet.
[485] *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen?, MR 2007, 342.
[486] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 5; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 120.
[487] *Klicka* in *Schwimann*, ABGB[3] II (2004) § 354 Rz 1.
[488] S dazu gleich Kap V.F.4.b).
[489] Dritte Richtlinie des Rates 78/855/EWG des Rates vom 9. Oktober 1978 gemäß Artikel 54 Absatz 3 Buchstabe g) des Vertrages betreffend die Verschmelzung von Aktiengesellschaften, ABl L 1978/295, 36.
[490] Sechste Richtlinie des Rates vom 17. Dezember 1982 gemäß Artikel 54 Absatz 3 Buchstabe g) des Vertrages bereffend die Spaltung von Aktiengesellschaften, ABl L 1982/378, 47.

Verschmelzungen und Spaltungen das Erfordernis einer entsprechenden Prüfung normieren.

Im österr Recht wird diesen Anforderungen durch die Bestimmungen der § 220b AktG (für Verschmelzungen) sowie § 5 Abs 1 SpaltG (für Spaltungen) entsprochen. § 220b AktG zufolge ist der Verschmelzungsvertrag für jede an der Verschmelzung beteiligte AG oder für alle gemeinsam durch einen Verschmelzungsprüfer zu prüfen.[491] Dagegen ist für eine übertragende GmbH eine Verschmelzungsprüfung nur dann vorgeschrieben, wenn diese von mindestens einem Gesellschafter verlangt wird.[492]

Bei einer Spaltung sieht § 5 SpaltG sowohl für die GmbH als auch die AG zwingend eine Prüfung für die auf- oder abspaltende Gesellschaft vor (wobei die Prüfung ausnahmsweise unterbleiben kann, wenn sämtliche Anteilsinhaber der spaltenden Gesellschaft darauf verzichten).[493] Somit wird iE in den meisten Fälle bereits aufgrund gesetzlicher Anordnung eine Prüfung der Umstrukturierung bzw die Durchführung einer Due Diligence geboten sein.

Weiters ist der Umstand zu beachten, dass eine Beiziehung von Sachverständigen für die mit der Akquisition befassten verantwortlichen Gesellschaftsorgane zumeist schon in Hinblick auf die Einhaltung des gesellschaftsrechtlichen Sorgfaltsmaßstabes angezeigt sein wird.[494] So wird bspw der Vorstand einer übernahmewilligen AG aus Überlegungen der unternehmerischen Vorsicht kaum ein anderes Mittel als eben die Beiziehung von Steuerberatern und insb Wirtschaftsprüfern haben, um sich ein ausreichend genaues Wissen über die Zielgesellschaft verschaffen zu können.

Nicht zuletzt auch das Risiko etwaiger schadenersatzrechtlicher Konsequenzen[495] (die sich bei gesellschaftsrechtlichen Umstrukturierungen nicht selten äußerst massiv darstellen können) und die Verantwortlichkeit gegenüber internen vorgesetzten Gremien

---

[491] *Kalss*, Verschmelzung – Spaltung – Umwandlung (1997) § 220b AktG Rz 4; *Szep* in *Jabornegg/Strasser* (Hrsg) AktG[4] (2006) § 220b Rz 5.

[492] § 100 Abs 2 GmbHG; ein Fall der wohl insb bei einem str Umtauschverhältnis eintreten wird; mwN *Koppensteiner/Rüffler*, GmbHG-Kommentar[3] (2007) § 100 Rz 6.

[493] *Duursma/Duursma-Kepplinger/Roth*, Handbuch zum Gesellschaftsrecht (2007) Rz 4462; mwN *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 241.

[494] Für D idZ sogar eine Verpflichtung aus aktienrechtlichen Gründen annehmend *Böttcher*, Verpflichtung des Vorstands einer AG zur Durchführung einer Due Diligence, NZG 2005, 54.

[495] § 84 Abs 2 AktG.

(zB Aufsichtsrat oder Aktionärsversammlung) wird für das entsprechende entscheidungsbefugte Organ die Durchführung einer Due Diligence sinnvoll machen.[496]

Aus datenschutzrechtlicher Sicht ist nun abzuklären welche Rolle den hierbei eingesetzten Prüfern nach dem Regime des DSG zukommt.[497] Wie gezeigt wurde ist bei der Durchführung einer Due Diligence in erster Linie der Eigentümer des Unternehmens als datenschutzrechtlicher Auftraggeber zu qualifizieren; ihm allein kommt die Entscheidung zu eine solche überhaupt erst zu veranlassen.[498] Der Eigentümer trifft also die Entscheidung die mit dem Unternehmen im Zusammenhang stehenden personenbezogenen Daten (mehrerer Betroffener) zum Zweck der Due Diligence zu verarbeiten. Dies entspricht der Legaldefinition des Auftraggebers in § 4 Z 4 DSG.

Für die rechtliche Qualifikation der bei der Due Diligence eingesetzten Prüfer ist zunächst zu untersuchen, ob deren Tätigkeit unter den datenschutzrechtlichen Begriff des Dienstleisters subsumiert werden kann.

Dienstleister iSd § 4 Z 5 DSG sind leg cit „natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden“. Als das herzustellende Werk lässt sich dabei ohne Schwierigkeiten der vom Verkäufer in Auftrag gegebene Due Diligence Prüfbericht qualifizieren.

Ob die Prüfungstätigkeit der beigezogenen Sachverständigen dabei als bloße Dienstleistertätigkeit einzuordnen ist, ist mE nach dem Grad des selbstständigen Agierens der befassten Prüfer im Umgang mit den personenbezogenen Daten zu beurteilen. Im interessierenden Fall wird die Selbstständigkeit der Prüfer jedoch nahezu ausnahmslos als sehr hoch anzunehmen sein.[499] Dies wird va daran liegen, dass es ja die

---

[496] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 17.
[497] Bedeutsam ist va, ob die Prüfer als Auftraggeber oder lediglich als Dienstleister nach dem DSG zu qualifizieren sind, da mit ersterer Eigenschaft zahlreiche Verpflichtungen einhergehen; vgl dazu insb §§ 14, 17 und 24 f DSG.
[498] S Kap V.F.4.a).
[499] IdS auch *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 238.

besonderen sachverständigen Fähigkeiten des Prüfers sind aufgrund derer seine Beauftragung überhaupt erst erfolgt ist.

Um im Gegenzug zu einer Qualifikation der Prüfer als Dienstleister zu kommen müssten mE die Anweisungen des die Due Diligence in Auftraggebenden dermaßen weitgehend inhaltlich ausgestaltet sein, dass dem Prüfer de facto kein Raum mehr für eigenständige Entscheidungen über Datenverarbeitungen mehr bliebe; ein Szenario das in der Praxis gesellschaftsrechtlicher Umstrukturierungen jedoch wenig wahrscheinlich ist, zumal wie erwähnt die eigenständige Prüfungsleistung aufgrund einer einschlägig juristisch/wirtschaftlichen Expertise wesentliche Grundlage für die Beauftragung mit der Erstellung des Due Diligence Prüfberichtes gewesen sein wird.

Gerade bei der Due Diligence liegt typischerweise einer jener Fälle von Beauftragungsverhältnissen vor, in denen traditionellerweise der Beauftragte selbständig (und somit „eigenverantwortlich“ iSd der datenschutzrechtlichen Diktion) über die Verwendung der ihm übergebenen Informationen entscheidet und hiezu auch nach den für ihn geltenden Standesregeln[500] verpflichtet und dafür auch verantwortlich ist.[501] Dabei sind es gerade Vertreter freier Berufe wie Rechtsanwälte oder Wirtschaftstreuhänder, die typischerweise bei bzw im Vorfeld der Due Diligence herangezogen werden.[502]

Die jeweils befassten Rechts-, Steuer- und sonstigen Berater treffen somit bei der Erstellung der geforderten Prüfberichte eindeutig eigenständige Entscheidungen über die Verarbeitung der durch das zu prüfende Unternehmen bereitgestellten personenbezogenen Daten.[503]

Die prüfenden Rechts- und Wirtschaftsberater sind mE daher jedenfalls als datenschutzrechtlicher Auftraggeber anzusehen. Ein weiteres Argument hierfür lässt sich schließlich dem Gesetzestext selbst entnehmen: Die im Zuge der Due Diligence vorgenommen Prüfungsschritte entsprechen in ihrer Tatbestandsmäßigkeit geradezu

---

[500] S dazu auch die Kap IV.B.9 und IV.B.10.
[501] Vgl dazu *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 114.
[502] *Berens/Hoffjan/Strauch* in *Berens/Brauner/Strauch* (Hrsg), Due Diligence bei Unternehmensakquisitionen[4] (2005) 139 (140).
[503] IglS *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence ?, MR 2007, 341.

idealtypisch den in § 4 Z 4 DSG letzter Satz beschriebenen Tätigkeiten.[504] Als bedeutendste Konsequenz dieses Umstandes sind es nun die Prüfer, die die datenschutzrechtlichen Melde- und Genehmigungspflichten zu beachten haben.[505]

Dieses Ergebnis (das wie dargestellt aufgrund der einschlägigen Bestimmungen des DSG entsprechend eindeutig scheint) ist mE jedoch nicht unproblematisch.

Es führt iE nämlich dazu, dass in der unternehmerischen Praxis spätestens mit Aufnahme der Prüfungstätigkeit die tatsächliche Auftraggebereigenschaft vom geprüften Unternehmen auf die Prüfer wechseln wird. Diesen obliegen ab diesem Zeitpunkt daher auch sämtliche datenschutzrechtlichen Meldepflichten.

Ein Umstand der sich bei umfangreichen Datenverarbeitungen aufgrund verschiedenartiger Prüfungsschwerpunkte nicht selten als äußerst aufwendig und va zeitintensiv auswirken dürfte. Insb existiert bis dato keine Standardanwendung, die derartige Meldungen deutlich vereinfachen und beschleunigen könnte.[506]

c) Der Käufer

Der datenschutzrechtliche Status des Käufers ist im Rahmen der Due Diligence im Vergleich zu jenem von Verkäufer und Prüfer verhältnismäßig passiv. Wie dargestellt wurde, kann dem Käufer jedenfalls nicht die Rolle des datenschutzrechtlichen Auftraggebers zugewiesen, werden – mag er auch derjenige sein, der das größte Interesse an der Due Diligence hat.[507]

Da der Käufer weder Auftraggeber iSd § 4 Z 4 DSG noch Betroffener iSd § 4 Z 3 DSG sein kann, kommt ihm vielmehr die Rolle eines Dritten zu, er befindet sich typischerweise außerhalb der Beziehung von Auftraggeber und Betroffenem. Zwar wird zwischen Käufer und den bei der Due Diligence eingesetzten Prüfern regelmäßig ein Vertragsverhältnis bestehen, bezüglich datenschutzrechtlicher Melde- und Auskunftspflichten ist dieses im Verhältnis zu den Betroffenen jedoch nicht von

[504] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 5.
[505] S Kap V.E.5.b).
[506] S dazu die Anlagen 1 und 2 der StMV aus denen sich keinerlei Anhaltspunkte für eine Anwendbarkeit im Falle einer Due Diligence ergeben.
[507] Kap V.F.4.a).

Bedeutung. Da der erstellte Prüfbericht (und somit auch alle darin verarbeiteten personenbezogenen Daten) schließlich an den Käufer weitergeleitet wird, wird iE allerdings eine Übermittlung iSd § 4 Z 12 DSG verwirklicht. Die Pflicht der Meldung solcher Übermittlungen beim DVR und Information der Betroffenen trifft jedoch stets den Auftraggeber der Datenverarbeitung.[508]

An dieser Stelle ist nochmals auf die aus datenschutzrechtlicher Sicht sehr bedeutsame Option des Käufers, nach Erhalt des Prüfberichtes von der Akquisition abzusehen, hinzuweisen. Ein durchaus denkbarer Fall, hat die Due Diligence doch gerade den Sinn etwaige „Deal Breaker" aufzudecken.[509] Diesfalls unterbleibt die Umstrukturierung und es kommt insb zu keiner Gesamtrechtsnachfolge.[510]

Gerade ein solches Verhalten des Käufers lässt mE einmal mehr die Argumentation jener, die Fragen der Einhaltung datenschutzrechtlicher Vorschriften nach vollzogener Umstrukturierung durch das Institut der Gesamtrechtsnachfolge als unproblematisch und damit Umstrukturierungsmaßnahmen als datenschutzneutral betrachten, für den unternehmerischen Alltag betriebswirtschaftlicher Entscheidungen als praxisfern und somit nicht als allgemein taugliche Lösung derartiger Problemstellungen erscheinen.[511]

5. Der Due Diligence Datenraum

Die eigentliche Prüfungsvorgang findet regelmäßig entweder im Zielunternehmen selbst oder in externen Räumlichkeiten wie bspw in der Kanzlei der mit der Due Diligence betrauten Wirtschaftsprüfer oder Rechtsanwälte statt.[512] Letztere Variante wird insb dann gewählt werden, wenn das Interesse besteht, eine anstehende Umstrukturierung vorerst noch nicht publik zu machen (bspw um eine Verunsicherung der Mitarbeiter zu vermeiden).[513]

---

[508] Kap V.F.4.b).
[509] *Hofmann*, Due Diligence – Grenzen und Möglichkeiten des Managements (2006) 24.
[510] Vgl dazu auch *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion: (k)ein Thema?, NJW 2002, 1542.
[511] S dazu Kap V.E.2.
[512] Vgl dazu *Berens/Hoffjan/Strauch* in *Berens/Brauner/Strauch* (Hrsg), Due Diligence bei Unternehmensakquisitionen[4] (2005) 124 f.
[513] IdS *Gran*, Abläufe bei Mergers und Acquisitions, NJW 2008, 1411.

Hierfür wird zumeist ein eigener Raum eingerichtet, in dem sämtliche relevanten Dokumente des Unternehmens zur Einsicht bereit gestellt werden; dies ist der sog Datenraum.[514] In Folge werden nun jene Aspekte beschrieben, die im Zuge gesellschaftsrechtlicher Umstrukturierungen aus datenschutzrechtlicher Perspektive besondere Relevanz besitzen.

a) Einrichtung und Organisation des Datenraumes

Vorerst ist abzuklären, ob der Datenraum physisch oder elektronisch zu organisieren ist. Gerade bei grenzüberschreitenden Umstrukturierungen mit Akquisitionsinteressenten in mehreren Ländern sind mittlerweile zunehmend Tendenzen zu elektronischen Datenräumen festzustellen.[515]

Zwar ist es hierbei unvermeidlich, die zu prüfenden Unterlagen vorerst physisch zusammenzustellen, der organisatorische Aufwand in den jeweiligen Ländern entsprechende Räumlichkeiten anzumieten sowie auch Mitarbeiter zu deren Beaufsichtigung bereitzustellen kann dafür unterbleiben. Einzig das entsprechende IT-Personal muss während der Due Diligence zur Verfügung stehen, was bei einem virtuellen Datenraum jedoch problemlos an einem einzigen Standort gewährleistet werden kann.[516]

Auch für die jeweiligen Kaufinteressenten bietet die Einrichtung eines elektronischen Datenraumes erhebliche Vorteile: Diesen und va auch deren Beratern im Rahmen der Due Diligence bleibt zum einen eine (möglicherweise kostenintensive) Anreise zum Zielunternehmen erspart, zum anderen sind sie zumeist nicht an zeitliche Vorgaben des Verkäufers bzw dessen Personals bei Einsicht in die zu prüfenden Unterlagen gebunden. Wie noch zu zeigen sein wird, muss elektronischen Datenräume nichtsdestotrotz sowohl in praktischer als auch spezifisch datenschutzrechtlicher Hinsicht nicht stets der Vorzug zu geben sein.

---

[514] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 106.
[515] Zu dieser Entwicklung allgemein *Sima/Uitz*, Zum Unternehmenskauf ins Internet, Die Presse vom 15.9.2008.
[516] *Kozak/Uitz*, Virtuelle Daten(t)räume, ecolex 2007, 440.

Im Hinblick auf das vom geprüften Unternehmen eingesetzte IT-Personal sind außerdem weitere datenschutzrechtliche Vorgaben zu beachten. Während die Einrichtung eines physischen Datenraums zumeist durch das umzustrukturierende Unternehmen selbst oder durch die Berater des Akquisitionsinteressenten erfolgen kann, werden bei der Erstellung elektronischer Datenräume üblicherweise eigens hierauf spezialisierte Unternehmen beigezogen.[517] Einer kurzen Behandlung der idZ interessierenden Fragestellungen widmet sich das folgende Kap.

(1) Beiziehung eines Dienstleisters bei der Einrichtung eines elektronischen Datenraums – Begriff und Funktion nach dem DSG

IdR wird das geprüfte Unternehmen mit dem Ersteller des Datenraums entsprechende vertragliche Vereinbarungen treffen, die regeln, wie bereitgestellte Unterlagen im elektronischen Datenraum zur Verfügung gestellt werden. Da dem mit der Einrichtung des elektronischen Datenraumes betrauten, Unternehmen die Daten lediglich überlassen werden, ist dieses mE als Dienstleister iSd § 4 Z 5 DSG zu beurteilen.[518] Insb trifft dieses (anders als die mit der Due Diligence befassten Prüfer) keine eigenständigen Entscheidungen über die Datenverarbeitung, auch eine Datenverwendung für eigene Zwecke scheint hier wenig wahrscheinlich.[519]

Ob ein Dienstleistungsverhältnis vorliegt oder nicht, ist datenschutzrechtlich von erheblicher Bedeutung: Werden Daten vom geprüften Unternehmen an den Datenraum-Dienstleister nur im Rahmen einer Überlassung weitergegeben, liegt damit keine Übermittlung iSd § 4 Z 12 DSG vor, weshalb iE auch die strengen Voraussetzungen für die Zulässigkeit einer Datenverwendung nach § 7 Abs 2 DSG nicht erfüllt werden müssen.[520] Abgesehen davon bestehen zwischen Auftraggeber und Dienstleister bestimmte Pflichten sowie die Erfordernis eine Dienstleistervereinbarung[521] abzuschließen.[522]

---

[517] *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen?, MR 2007, 342.
[518] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 6.
[519] Offensichtlich aA *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen?, MR 2007, 342; eigenständige Entscheidungen über die Art und Weise der Datenverwendung sind mE jedoch deshalb wenig wahrscheinlich, da Ausmaß und Handhabung der offenzulegenden Unterlagen idR bereits durch eine entsprechend detaillierte Vereinbarung zwischen Verkäufer und Käufer festgelegt sein werden.
[520] § 4 Z 11 iVm § 7 Abs 2 DSG.
[521] § 10 Abs 1 DSG.
[522] *Knyrim*, Datenschutzrecht (2003) 191.

(2) Die Bedeutung des Sitzes des Datenraum-Dienstleisters

Erhebliche Bedeutung kommt dem Umstand zu, wo der Datenraum-Dienstleister seinen Sitz hat. Soweit dieser in einem Mitgliedstaat der EU (bzw des EWR)[523] gelegen ist, ist (bei einer bisher zulässigen Verarbeitung) die Datenüberlassung unbedenklich. [524]

Befindet sich der Sitz des Datenraum-Dienstleisters dagegen in einem Drittland stellt sich die Situation grundlegend anders dar. Diesfalls ist zu prüfen, ob materielle Gründe wie eine Zustimmung der Betroffenen oder die Notwendigkeit zur Vertragserfüllung die Datenüberlassung gestatten. Weiters, ob diese in ein hinsichtlich seines Datenschutzniveaus der EU gleichgestelltes Land erfolgt, oder, ob Standardvertragsklauseln[525] für Auftragsverarbeiter abgeschlossen wurden. In allen Fällen ist jedoch grds eine Genehmigung der Datenüberlassung durch die DSK erforderlich.[526] Eine eingehendere Untersuchung der Fragestellungen iZm dem grenzüberschreitenden Verkehr personenbezogener Daten wird in Kap V.F. gegeben.

b) Geheimhaltung und Kontrolle

Bei einem physischen Datenraum werden (personen- wie nicht personenbezogene) geheimhaltungspflichtige Daten typischerweise durch eine entsprechende Vereinbarung geschützt.[527] Diese ist von den Prüfern im Hinblick auf die Vertraulichkeit der von ihnen einzusehenden Prüfungsunterlagen zu unterzeichnen.

Auch die Vereinbarung entsprechender Datenraumregeln zwischen dem geprüften und dem akquisitionswilligen Unternehmen ist anzuraten (und auch weitgehend Praxis); in Betracht können dabei ebenso Regelungen zur Zulässigkeit von Anfragen und die Festlegung von Öffnungs- bzw Zugangszeiten wie die Untersagung der Anfertigung von Kopien oder Nutzung von Foto-Handys kommen.[528]

---

[523] Vgl dazu *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 12 Anm 2.
[524] § 12 Abs 1 DSG.
[525] E der Kommission vom 27.12. 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG, ABl L 2002/6, 52.
[526] IdS *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 12 Anm 3; *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen?, MR 2007, 343; aA *Knyrim*, Datenschutzrecht (2003) 193.
[527] *Heidinger/Albeseder*, Due Diligence, Ein Handbuch für die Praxis (2001) 19; *Gran*, Abläufe bei Mergers und Acquisitions, NJW 2008, 1410.
[528] *Gran*, Abläufe bei Mergers und Acquisitions, NJW 2008, 1411.

Als Vorteil dieser konventionellen Variante stellt sich in erster Linie die Kontrolle der tatsächlich Einsichtnehmenden dar: In einem physischen Datenraum ist durch entsprechende Kontrollen an den Eingängen sowie das Führen von Aufzeichnungen eine Überprüfung der jeweils Anwesenden ohne Schwierigkeiten zu bewerkstelligen.[529]

Bei elektronischen Datenräumen dagegen erfolgt der „Eintritt" in den Datenraum idR durch Eingabe eines Zugangspasswortes, ob die nun solcherart eingeloggte reale Person aber tatsächlich zur Einsicht autorisiert ist oder nicht, kann dabei nicht mit Sicherheit festgestellt werden. Im Verhältnis zwischen der geprüften Gesellschaft und dem beigezogenen Datenraum-Dienstleister ist weiters auf dessen Verpflichtung zur Einhaltung der in § 11 Abs 1 DSG demonstrativ[530] normierten Pflichten hinzuweisen. Diese Pflichten des Dienstleisters bestehen zwar grds bereits kraft Gesetz, aus Gründen der Rechtsicherheit wird sich die Erstellung eines schriftlichen Vertrages mE aber stets empfehlen.[531]

Ebenfalls problematisch erscheint der Umstand, das bei Nutzung eines elektronischen Datenraums eine Aufzeichnung des jeweiligen Nutzerverhaltens möglich bzw aus der Protokollierungspflicht gem § 14 Abs 2 Z 7 DSG geboten ist.[532] Ziel dieser Protokollierungspflicht ist es, Datenanwendungen nachvollziehbar zu machen, um deren Rechtmäßigkeit zu prüfen und die Rechte von Betroffenen zu wahren.[533]

IZm den Vorschriften zur Datensicherheit ist außerdem auf den Umstand hinzuweisen, dass gem § 14 Abs 3 DSG Übermittlungen für nicht registrierte Datenanwendungen so zu protokollieren sind, dass dem Betroffenen Auskunft nach § 26 Abs 1 DSG erteilt werden kann.[534] Da keine entsprechenden Musteranwendungen existieren ist mE daher von einer entsprechenden Protokollierungspflicht auszugehen. Zu beachten ist, dass bei

---

[529] *Kozak/Uitz*, Virtuelle Daten(t)räume, ecolex 2007, 441.
[530] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 11 Anm 1; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 56.
[531] IglS *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 11 Anm 3; s auch die diesbezügliche Anordnung in § 11 Abs 2 DSG, die jedoch erst für die „nähere Ausgestaltung" der Pflichten des Dienstleisters ein schriftliches Festhalten erfordert.
[532] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 14 Anm 12.
[533] *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 93; im Hinblick auf Überlegungen zur Datensicherheit iZm der Datenüberlassung an den Datenraum-Dienstleister vgl auch *Knyrim*, Datenschutzrecht (2003) 230.
[534] VfGH B 227/05 VfSlg 18230.

einer fahrlässig unterlassenen Registrierung der Due Diligence eine nachträglich erforderlich gewordene Dokumentation einen erheblicher Aufwand bedeuten kann.[535]

Abgesehen vom Umstand, dass die Prüfer dabei selbst zu datenschutzrechtlich Betroffenen werden können, sind va die Erkenntnisse die sich aus ihrer Tätigkeit für den Geprüften gewinnen lassen können bedeutsam.[536] So kann etwa das Interesse für einen bestimmten Unternehmensbereich oder bestimmte Lieferanten- und Kundenbeziehungen Rückschlüsse über die Akquisitionsstrategie des Kaufinteressenten geben. Die Gewinnung derartiger Informationen (so unvermeidbar diese in der Praxis auch anfallen mögen) wird sich mE nur schwerlich mit dem Kontrollzweck nach § 14 Abs 4 DSG in Einklang bringen lassen, der va auf den Schutz (und nicht die Kontrolle)[537] der Betroffenen gerichtet ist.

Um diesbezüglich unliebsame Konsequenzen aus datenschutzrechtlichen Verstößen zu vermeiden wird es idR ratsam sein entsprechende Zustimmungserklärungen der Prüfer bereits vorab einzuholen. [538]

c) Prüfung der Unterlagen – Konsequenzen für Gewährleistungsansprüche

Neben den in Kap V.E.5.a) aufgezeigten Vorteilen eines elektronischen Datenraums sind jedoch auch Nachteile zu berücksichtigen, die sich mangels physisch verfügbarer Prüfungsunterlagen ergeben können. So kann durch lange Wartezeiten beim Laden von Dokumenten eine Kostenerhöhung eintreten; ebenso kann sich für den Akquisitionsinteressenten die Durchführung einer Due Diligence in den eigenen Arbeitsräumlichkeiten durch übliche Störungen während eines normalen Arbeitstages als unvorteilhaft erweisen. Des weiteren wird auch der Informationsaustausch zwischen einzelnen Gruppen von Beratern aufgrund der getrennten Arbeit in den eigenen Räumlichkeiten erschwert.[539]

---

[535] Vgl dazu auch *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 95.
[536] Zur datenschutzrechtlichen Auftraggebereigenschaft der Prüfer idZ s Kap V.E.4.b).
[537] Vgl *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 14 Anm 17.
[538] *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen?, MR 2007, 345.
[539] *Kozak/Uitz*, Virtuelle Daten(t)räume, ecolex 2007, 441.

Freilich sind dies keine spezifisch (datenschutz-) rechtlichen Argumente gegen die Durchführung der Due Diligence in elektronischer Form, nichtsdestotrotz kommt derartigen faktischen Umstände in der unternehmerischen Praxis erhebliche Bedeutung zu weshalb sie entsprechend zu berücksichtigen sind.

Die Prüfung der vom Zielunternehmen zur Verfügung gestellten Daten hat insb für etwaige Gewährleistungsansprüche maßgebliche Bedeutung.[540] Einmal im Rahmen der Due Diligence offengelegte und geprüfte Unterlagen sind als Grundlage eines Gewährleistungsanspruches grds nicht mehr tauglich.[541]

Diesbezüglich wird das geprüfte Unternehmen auch meist eine Vereinbarung anstreben, wonach der gesamte Datenrauminhalt als offengelegt und dem Akquisitionsinteressenten bekanntgemacht gilt; eine Regelung, die für letzteren jedoch insb bei einem elektronischen Datenraum insofern nachteilig sein kann, als er Schwierigkeiten haben kann in einem verhältnismäßig kurzen Zeitraum den gesamten Inhalt zu überblicken und somit alle erdenklichen Risiken und Mängel der Akquisition zu berücksichtigen.

Eine Kompromisslösung könnte bspw darin bestehen, jene Unterlagen als offengelegt anzusehen, die der Käufer auch tatsächlich geprüft hat. Dieser wird jedoch zumeist kein gesteigertes Interesse an einer derart genauen Aufzeichnung seines Datenraumverhaltens haben weshalb entsprechende Vereinbarungen in der unternehmerischen Praxis iE wohl nur sehr selten denkbar sind.[542]

d) Maßgeblicher Inhalt des Datenraums

Um die soeben dargestellten Gewährleistungsansprüche überprüfen zu können, muss sich verbindlich feststellen lassen welche Unterlagen nun tatsächlich Gegenstand der Due Diligence Prüfung waren.

---

[540] *Parschalk/Wahl*, Ausgewählte Fragen der Gewährleistung beim Unternehmenskauf, wbl 2003, 353; mwN *Picot* in *Berens/Brauner/Strauch* (Hrsg) Due Diligence bei Unternehmensakquisitionen[4] (2005) 331.

[541] Vgl idZ auch die allgemein Gewährleistungsregelung des § 928 ABGB.

[542] IdS *Kozak/Uitz*, Virtuelle Daten(t)räume, ecolex 2007, 442.

In einem konventionellen Datenraum werden dafür die offen gelegten Ordner nach Überprüfung des Inhaltes durch Vertreter von sowohl des geprüften als auch des akquisitionswilligen Unternehmens begutachtet, in Kartons verpackt und schließlich von einem Notar verschlossen und versiegelt und zumindest für die Dauer der im Akquisitionsvertrag festgelegten Gewährleistungsfrist treuhändig verwahrt.[543]

Im Falle eines elektronischen Datenraumes kommt eine Speicherung des Datenrauminhaltes auf einem entsprechenden Datenträger in Betracht. Auch hierbei empfiehlt sich eine Überprüfung des gespeicherten Inhaltes durch Vertreter beider Parteien.

In beiden Varianten sollte sich bei Einhaltung dieser Vorgangsweisen in einem allfälligen Streitfall damit der Beweis, welche Unterlagen nun tatsächlich offengelegt wurden idR als problemlos erweisen.

6. Die Weitergabe des Due Diligence Prüfberichts – datenschutzrechtliche Vorgaben und Erfordernisse

Wie bereits mehrfach dargelegt sind die im Rahmen der Due Diligence gewonnen Informationen für den Akquisitionsinteressenten von elementarer Bedeutung. Lassen nun die mit der Due Diligence Prüfung betrauten Berater (als datenschutzrechtliche Auftraggeber) ihren idZ erstellten Bericht (bzw die darin verarbeiteten personenbezogenen Daten) dem potentiellen Erwerber des Zielunternehmens (als Drittem) zukommen, ist darin eine Übermittlung iSd § 4 Z 12 DSG zu sehen.

Zur generellen datenschutzrechtlichen Zulässigkeit der Übermittlung wird auf die diesbezüglichen Ausführungen in Kap V.D.3. verwiesen. Im Anschluss werden nur spezifische Fragestellungen im Hinblick auf die im Due Diligence Prüfbericht verarbeiteten Daten erörtert, insb sind die unterschiedlichen datenschutzrechtlichen Vorgaben im Hinblick auf nicht-sensible und sensible Daten darzustellen.

---

[543] *Kozak/Uitz*, Virtuelle Daten(t)räume, ecolex 2007, 442; vgl dazu auch *Berens/Hoffjan/Strauch* in *Berens/Brauner/Strauch* (Hrsg) Due Diligence bei Unternehmensakquisitionen[4] (2005) 163.

a) Die Übermittlung nicht-sensibler Daten

Ob die Übermittlung des erstellten Prüfberichts zulässig ist, ist nach § 7 Abs 2 DSG zu beurteilen. § 7 Abs 2 Z 1 DSG verweist hierbei vorerst auf § 7 Abs 1 DSG: dies bedeutet iE, dass nur solche Daten verwendet werden dürfen, die aus einer nach Abs 1 der Bestimmung zulässigen Datenanwendung stammen.[544]

Zweck und Inhalt des Due Diligence Berichtes werden für gewöhnlich problemlos zu eruieren sein; als nächster Schritt muss eine Deckung durch rechtliche Befugnisse des jeweiligen Auftraggebers vorhanden sein. Eine solche im vorliegenden Fall zu finden scheint prima facie gewisse Schwierigkeiten zu verursachen – im privaten (idZ privatwirtschaftlichen) Bereich wird sich eine solche zumeist aus einer Gewerbeberechtigung, Konzessionen eines Unternehmens nach spezifischen Materiengesetzen oder dem Gesellschaftsvertrag eines Unternehmens ableiten lassen.[545]

Aber auch wenn vorerst keine, explizit auf die Übermittlung von Due Diligence Prüfberichten abstellende, rechtliche Befugnis ersichtlich ist, wird eine solche meiner Auffassung nach dennoch anzunehmen sein, da als Prüfungsmaßstab nicht nur eine konkrete Berechtigung, sondern die Rechtsordnung als Gesamtheit heranzuziehen ist.[546] Unter Berücksichtigung der Rechtsgrundlage des allgemeinen Gebarens des Unternehmens (die eben bspw ein Gesellschaftsvertrages darstellen kann) werden sich Verfahren wie Due Diligence Prüfungen im Vorfeld geplanter Umstrukturierungen als nicht unübliche Vorgänge betriebswirtschaftlicher Praxis mE zumindest mittelbar rechtfertigen lassen.

Als weitere Voraussetzung für die Zulässigkeit der Übermittlung fordert § 7 Abs 2 Z 2 DSG, dass der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis (soweit diese nicht außer Zweifel steht) im Hinblick auf den Übermittlungszweck glaubhaft macht.

Da die Due Diligence Prüfer regelmäßig im Auftrag des Akquisitionsinteressenten tätig werden, kann dessen rechtliche Befugnis zur Verwendung der Daten jedoch mE iSd des

---

[544] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 7 Anm 8.
[545] *Knyrim*, Datenschutzrecht (2003) 94.
[546] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 7 Anm 5.

Gesetzeswortlautes als außer Zweifel stehend betrachtet werden. Einer Übermittlung des Prüfberichts kann die Bestimmung iE daher nicht entgegenstehen.

Schließlich dürfen gem § 7 Abs 2 Z 3 DSG durch Zweck und Inhalt der Übermittlung (ebenso wie bei der Verarbeitung) keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden. Diesbezüglich ist § 8 DSG maßgeblich.

Ob schutzwürdige Interessen der von der Übermittlung Betroffenen verletzt sind, ist durch eine Interessenabwägung zu prüfen.[547] Eine solche im Einzelfall[548] vorzunehmen, dürfte in der Praxis jedoch erhebliche Schwierigkeiten verursachen. In Bezug auf Mitarbeiterdaten wird es mE zumindest denkbar sein bei bestimmten, insb gleichartigen Arbeiternehmergruppen für die Interessenabwägung jeweils einen „Norm-Mitarbeiter" heranzuziehen und das Ergebnis als repräsentativ für die gesamte Gruppe personenbezogener Daten zu werten. Anstatt einer Einzelprüfung jeder Mitarbeiterbeziehung wird sich dagegen auch eine summarische Prüfung iE als durchaus sachgerecht erweisen können.[549]

In einer Gesamtschau dürfte die Interessenabwägung bei der Übermittlung personenbezogener Daten im Rahmen einer Umstrukturierung tendenziell zugunsten einer Zulässigkeit ausschlagen. Insb besteht die Notwendigkeit potentiellen Akquisitionsinteressenten eine entsprechend genaue Information über das Zielunternehmen geben zu können. Abgesehen davon lässt auch die Rechtsordnung als solche durch ihre Bestimmungen[550] zu gesellschaftsrechtlichen Umstrukturierungen erkennen, dass diese grds erwünscht und daher erleichtert werden sollen. Daher wird iE zumeist von der Zulässigkeit derartiger Übermittlungen auszugehen sein.[551]

Deutliche Einschränkungen ergeben sich jedoch bei der Übermittlung sensibler Daten. Hier ist den wesentlich strengeren Erfordernisse des § 9 DSG zu entsprechen.

---

[547] § 8 Abs 1 Z 4 DSG; s dazu auch *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 7 Anm 10.
[548] Vgl *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 240.
[549] IdS *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion – (k)ein Thema?, NJW 2002, 1542.
[550] Vgl dazu bspw §§ 96 ff GmbHG und §§ 219 ff AktG.
[551] IdS auch – zwar außerhalb des Datenschutzrechtes, im Hinblick auf spezifische Geheimhaltungsvorschriften jedoch von vergleichbarer Wertung – *Nowotny*, „Due Diligence" und Gesellschaftsrecht, wbl 1998, 145.

b) Die Übermittlung sensibler Daten

Unter den Begriff der sensiblen Daten fallen Informationen über rassische und ethnische Herkunft, politische Meinung und Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung sowie Gesundheit und Sexualität natürlicher Personen.[552]

(1) Spezifische Problematik

Im Rahmen einer Due Diligence wird eine Zulässigkeit der Übermittlung sensibler Daten aufgrund der taxativen Aufzählung des § 9 DSG zumeist nur bei Vorliegen einer entsprechenden Zustimmung des Betroffenen gegeben sein. Im Gegensatz zur Zustimmung bei der Verwendung nicht-sensibler Daten muss die Zustimmung allerdings ausdrücklich erfolgen. Dies bedeutet iE, dass auch dann, wenn mit dem Betroffenen ein Vertragsverhältnis besteht, eine Zustimmung ausdrücklich eingeholt werden muss.[553] Wie bereits aufgezeigt, wird die Einholung sämtlicher erforderlicher Zustimmungen vor Übermittlung des Prüfberichts nur sehr schwierig möglich, wenn nicht überhaupt undurchführbar sein.

Des weiteren ist im Gegensatz zur Verhältnismäßigkeitsprüfung bei nicht-sensiblen Daten insb der Rechtfertigungsgrund überwiegender berechtigter Interessen des Auftraggebers oder eines Dritten nicht vorgesehen (womit auch die sonst im Rahmen der Due Diligence meist zum gewünschten Ergebnis führende Interessensabwägung nicht herangezogen werden kann).

Selbst wenn daher die Verwendung sensibler Daten zur Erfüllung eines Vertragsverhältnisses notwendig ist, dürfen diese nicht ohne Zustimmung des Betroffenen verarbeitet werden, soweit die Verwendung nicht von den in § 9 DSG taxativ aufgezählten Gründen erfasst ist.[554]

---

[552] § 4 Z 2 DSG; zu den speziell im unternehmerischen Kontext in Betracht kommenden Daten s die Kap V.C.2. und V.E.2.
[553] *Knyrim*, Datenschutzrecht (2003) 109.
[554] OGH 29.6.2008, 6 ObA 1/06z.

(2) Lösungsvorschlag

Die praktikabelste Lösung dieses Problems besteht meiner Auffassung nach darin, den Personenbezug der Daten zu eliminieren.[555] Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten dann nicht verletzt, wenn die Daten in nur indirekt personenbezogener Form verwendet werden. Indirekt personenbezogen sind Daten dann, wenn der Personenbezug der Daten derart ist, dass ein Auftraggeber, Dienstleister oder Empfänger einer Übermittlung die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.[556]

Dies könnte bspw bereits das Zielunternehmen durch eine Verschlüsselung der für die Due Diligence zurverfügunggestellten personenbezogenen Daten erreichen. Die Prüfer der Due Diligence hätten dabei in dieser Phase keinen Zugriff auf den vom geprüften Unternehmen verwahrten Schlüssel und somit auch kein legales Mittel zu Feststellung der Identität der Betroffenen. Auch eine völlige Anonymisierung der Daten ist denkbar, hierbei kann niemand mehr die Daten auf eine in ihrer Identität bestimmte Person zurückführen.[557] Diesfalls wären überhaupt keine datenschutzrechtlichen Vorgaben mehr zu beachten, da anonyme Daten nicht als personenbezogene Daten iSd DSG gelten.[558]

Eine solche Beseitigung dürfte im Gros der Fälle auch für den Akquisitionsinteressenten vertretbar sein; so wird dieser zwar ein nachvollziehbares Interesse daran haben, zu erfahren, wie viele seiner potentiellen neuen Mitarbeiter bspw besonderen gesetzlichen Kündigungsschutz genießen, ein berechtigtes Interesse zu erfahren, ob es nun konkret „Frau X“ oder „Herr Y“ ist, die eine entsprechende Behinderung besitzen, dürfte dagegen idR nicht gegeben sein.

Anders kann sich die Situation dagegen bei Organmitgliedern und Führungskräften des Zielunternehmens darstellen. Diesfalls sind genaue Informationen über das Management oftmals von vitalem Interesse für den Kaufinteressenten. Hierbei dürfte

---

[555] IglS *Braun/Wybitul*, Übermittlung von Arbeitnehmerdaten bei Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 786; *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 240; *Fleischer/Körber* in *Berens/Brauner/Strauch* (Hrsg) Due Diligence bei Unternehmensakquisitionen[4] (2005) 296.
[556] § 9 Z 2 DSG.
[557] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 4 Anm 2.
[558] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 2.

sich jedoch der, durch die Einholung entsprechender Zustimmungen bedingte Aufwand auf die Information einiger weniger Betroffener beschränken und somit insgesamt nicht wesentlich ins Gewicht fallen.

Zusammenfassend wird sich bei der Übermittlung sensibler Daten mE daher eine Eliminierung der Personenbezuges sowie die in Einzelfällen gebotene Einholung der Zustimmung der Betroffenen sowohl als datenschutzkonform als idR auch die Due Diligence Prüfer (bzw das geprüfte Unternehmen) nicht über Gebühr organisatorisch belastend darstellen.

F. Besonderheiten grenzüberschreitender Umstrukturierungen

Da sich Unternehmenskäufe und –zusammenschlüsse am europäischen Binnenmarkt oft als geographisch wie rechtlich länderübergreifend darstellen, ist zu untersuchen welche Auswirkungen dieser Umstand auf datenschutzrechtlicher Ebene haben kann.

1. Problemaufriss

Wie gezeigt wurde, kommt es bei gesellschaftsrechtlichen Umstrukturierungen regelmäßig zu einer Verwendung personenbezogener Daten.[559] Als besonders häufig auftretenden Tatbestand des DSG ist idZ auf die Übermittlung iSd § 4 Z 12 DSG hinzuweisen. Übermittlungen und Überlassungen von personenbezogenen Daten ins Ausland sind hierbei nur unter den Voraussetzungen der §§ 12 und 13 DSG zulässig.

Insb der Informationsfluss im Zuge von Due Diligence Prüfungen findet dabei in der überwiegenden Zahl der Fälle auch grenzüberschreitend statt, und während dieser im Rahmen von Unternehmensakquisitionen im EU-Raum datenschutzrechtlich zumindest teilweise privilegiert[560] ist, stellt sich eine rechtskonforme Übermittlung personenbezogener Daten in Drittstaaten dagegen als ungleich komplizierter dar.

Hier ist auf zahlreiche Erfordernisse des DSG Bedacht zu nehmen. Dieses unterscheidet grds zwischen genehmigungsfreien[561] und genehmigungspflichtigen[562] Übermittlungen

[559] S Kap V.
[560] Dies freilich ungeachtet der grds Meldepflicht für jede sonstige Datenanwendung nach § 17 DSG.
[561] § 12 DSG.

und Überlassungen personenbezogener Daten ins Ausland. Diese, gerade bei grenzüberschreitenden Übermittlungen im Zuge von Unternehmensakquisitionen sehr bedeutsamen, Regelungen sind dabei durch eine Vielzahl von Verweisen gekennzeichnet und teils sehr komplex formuliert. Dies wirkt sich iE bedauerlicherweise sehr zu Lasten der Verständlichkeit und somit der beteiligten Unternehmen aus.

Auch bei Umstrukturierungen, bei denen die Zielunternehmen ausschließlich im europäischen Binnenmarkt gelegen sind, können sich durch die Beiziehung von Dienstleistern (wie eben zB für die Einrichtung eines elektronischen Datenraums) oder Outsourcingmaßnahmen[563] zahlreiche datenschutzrechtlich beachtliche Sachverhalte ergeben. Im Anschluss werden nun die unterschiedlichen datenschutzrechtlichen Anforderungen an Übermittlungen in EU-Mitgliedstaaten einerseits und Drittstaaten andererseits untersucht.

2. Datenverwendung im europäischen Binnenmarkt

Bezüglich der Datenübermittlung in EU-Mitgliedsstaaten enthält die Bestimmung des § 12 DSG sowohl eine territoriale als auch eine der Sitzstaattheorie (dazu gleich) entsprechende Anwendungsregelung.

a) Inlandsbezug als Anwendungsregelung

Ganz grds gilt das DSG für die Verwendung personenbezogener Daten im Inland.[564] Dh dass idR auf jede Datenverwendung in Österreich österreichisches Recht anzuwenden ist – ein Grundsatz in dem sich zumindest auch vereinzelte Elemente eines Territorialitätsprinzips erkennen lassen. Auch dieses entspricht iwS einem Anliegen der RL 95/46/EG, wonach auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaates Anwendung finden sollen.[565]

---

[562] § 13 DSG.
[563] Vgl dazu *Knyrim*, Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach! Ecolex 2009, 85.
[564] § 3 Abs 1 erster Satz DSG.
[565] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 19.

So steht bei der in § 3 Abs 1 DSG normierten Anknüpfung an einen Verwendungszwecks für eine Niederlassung des Auftraggebers in Österreich deutlich das Abstellen auf einen örtlichen Schwerpunkt der Datenverwendung im Vordergrund (und iE somit eine grds territoriale Rechtsanwendungsregelung).

In jedem Fall ist Rechtslücken vorzubeugen, die sich für Umgehungsstrategien anbieten, außerdem muss ein konkurrierender Regelungsanspruch von Rechtsordnungen mehrerer Mitgliedstaaten vermieden werden.[566] Um diesen Anforderungen gerecht zu werden findet sich in § 3 Abs 2 DSG eine weitere Anwendungsregelung; diese stellt im Gegensatz zu einem Inlandsbezug der Datenverwendung auf die Niederlassung des Auftraggebers ab.

b) Das datenschutzrechtliche Sitzstaatprinzip

Das sog Sitzstaatprinzip orientiert sich an den Betriebsstätten bzw Niederlassungen eines Unternehmens.[567] ME werden die meisten datenschutzrechtlichen Fragestellungen zum räumlichen Anwendungsbereich nach diesem Prinzip zu lösen sein. Dies liegt va an den zumeist grenzüberschreitenden wirtschaftlichen Hintergründen gesellschaftsrechtlicher Umstrukturierungen am europäischen Binnenmarkt; diesen wird im Gros der Fälle somit auch der Zweck der Datenverwendung in das Regime anderer EU-Mitgliedstaaten folgen. Nicht zuletzt geht auch die RL 95/46/EG als europarechtliche Vorgabe grds vom Sitzstaatprinzip aus.[568]

Das DSG ist somit auch für Datenanwendungen in anderen Mitgliedstaaten anwendbar, wenn diese für Zwecke einer Haupt- oder Zweigniederlassung eines österreichischen Unternehmens vorgenommen werden.[569]
Andererseits ist das Recht eines anderen Mitgliedstaates in Österreich für solche Datenanwendungen anzuwenden, die für Zwecke einer Haupt- oder Zweigniederlassung eines Unternehmens aus einem anderen Mitgliedstaat vorgenommen werden.[570]

---

[566] S die ErwG 18-21 sowie Art 4 RL 95/46/EG; vgl dazu auch *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 127.
[567] Vgl ErläutRV 1613 BlgNR 20. GP 36.
[568] Zu diesem Umstand s auch allgemein *Gola/Schomerus*, dBDSG[9] (2007) § 1 Rz 27.
[569] § 3 Abs 1 zweiter Satz DSG.
[570] § 3 Abs 2 DSG.

Voraussetzung für eine solche grenzüberschreitende Anwendbarkeit der Datenschutzgesetze ist dabei, dass im jeweiligen Zielland, dh jenem Land aus dem die personenbezogene Daten ua „stammen“ und in dem die Daten verarbeitet werden, keine eigene Zweigniederlassung besteht, für deren Zwecke die Daten verarbeitet werden.[571]

Va die „Niederlassung“ nach § 4 Z 15 DSG ist wesentlicher Anknüpfungspunkt für den räumlichen Anwendungsbereich des DSG im europäischen Binnenmarkt; darunter ist leg cit „jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.“, zu verstehen. Die Rechtsform der Niederlassung spielt somit keine Rolle; da für die Ausübung von Tätigkeiten ein Mindestmaß an personeller Infrastruktur erforderlich sein wird, wird bspw eine bloße Briefkastenfirma keine Niederlassung iSd § 4 Z 15 DSG begründen können.[572]

IZm gesellschaftsrechtlichen Umstrukturierungen ist insb darauf hinzuweisen, dass der Sitzbegriff des DSG ein anderer als jener des Gesellschaftsrechts ist. So ist nach der (in Kontinentaleuropa geltenden) gesellschaftsrechtlichen Sitztheorie Personalstatut einer juristischen Person das Recht jenes Landes, in dem die juristische Person ihren tatsächlichen Verwaltungssitz hat.[573] Für eine Anwendbarkeit des österr DSG allein ausschlaggebend ist dagegen nur der Umstand, dass die Datenverarbeitung für Zwecke einer in Ö gelegenen Niederlassung erfolgt.

Wie das DSG in § 4 Z 15 DSG klarstellt kommt es insb nicht auf das Vorliegen von Rechtspersönlichkeit des Auftraggebers an (auch wenn solche Fälle in der wirtschaftlichen Praxis idR selten seine dürften)[574], weshalb die jeweilige Anwendbarkeit von nationalen datenschutz- und gesellschaftsrechtlichen Vorschriften iE nicht zwingend kongruent sein muss.

---

[571] *Knyrim*, Datenschutzrecht (2003) 13.
[572] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 16; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 19; mwN *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 128.
[573] *Ratka*, Sitztheorie, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) 282; *Kalss*, Verschmelzung-Spaltung-Umwandlung (1997) § 219 AktG Rz 5; *Koppensteiner/Rüffler*, GmbHG-Kommentar[3] (2007) Einleitung Rz 17; *Verschraegen* in *Rummel*, ABGB[3] II/2 (2004) § 10 IPRG Rz 2; *Neumayr* in *Koziol/Bydlinski/Bollenberger*, ABGB[2] (2007) § 10 IPRG Rz 1.
[574] Gegebenenfalls wird jedoch bspw auch eine GesBR als datenschutzrechtlicher Auftraggeber zu qualifizieren sein.

3. Datenverwendung außerhalb des europäischen Binnenmarktes – Grundsatz der Genehmigungspflicht

Während der Ort der Niederlassung des Auftraggebers der maßgebliche Anknüpfungspunkt für die Frage des anwendbaren Rechts ist (soweit es sich um Datenanwendungen für einen Rechtsträger mit Sitz in einem EU-Mitgliedstaat handelt) gilt bei Datenanwendungen für Zwecke eines Rechtsträgers, der keinen Sitz in einem EU-Mitgliedstaat hat, immer der Ort der Datenverwendung als Anknüpfungspunkt für die Anwendbarkeit einer nationalen Rechtsordnung.[575]

Um die praktische Durchsetzbarkeit des jeweiligen einzelstaatlichen Rechts zu gewährleisten, hat der Auftraggeber der Datenverwendung einen verantwortlichen Vertreter[576] zu benennen, der (unbeschadet der Möglichkeit der Inanspruchnahme des Auftraggebers selbst) die datenschutzrechtliche Verantwortung trägt.[577] Diesem gegenüber kann dann die jeweilige nationale Kontrollstelle (für Österreich somit die DSK) ihre Befugnisse ausüben, ohne auf territoriale Kompetenzgrenzen zu stoßen.[578]

Solche Übermittlungen und Überlassungen personenbezogener Daten an Empfänger außerhalb des europäischen Binnenmarktes bedürfen zusätzlich stets einer Meldung und in weiterer Folge Genehmigung der DSK.[579] Die praktische Relevanz dieser Vorgaben ist nicht gering zu schätzen, haben doch bspw viele Unternehmen der EU wirtschaftliche (und damit auch gesellschaftsrechtliche) Akquisitionsinteressen im nahen osteuropäischen Raum.

Es ist jedoch darauf hinzuweisen, dass von der in § 13 Abs 1 DSG grds normierten Meldepflicht einige Ausnahmen bestehen; diese entsprechen dabei inhaltlich großteils den Ausnahmen der §§ 8 und 9 DSG.[580] Für Unternehmen idZ insb beachtenswert ist der Umstand, dass die Übermittlung von Daten die sich auf juristische Personen beziehen (im wesentlichen daher Wirtschaftsdaten) in EU-Mitgliedstaaten genehmigungsfrei ist. Dies, obwohl sich die RL 95/46/EG auf den Schutz von

---

[575] ErläutRV 1613 BlgNR 20. GP 36.
[576] § 6 Abs 3 DSG.
[577] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 20; vgl Art 4 Abs 1 lit c RL 95/46/EG.
[578] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 130.
[579] *Knyrim*, Datenschutzrecht (2003) 126.
[580] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 59.

natürlichen Personen beschränkt und die Mehrheit der Mitgliedstaaten keine Regelungen zum Schutz juristischer Personen kennen.[581]

a) Materielle Ausnahmen von der Genehmigungspflicht nach dem DSG

§ 12 Abs 3 DSG zählt abschließend zehn Fälle auf, in denen Datenübermittlungen- oder -überlassungen in Drittstaaten ohne Genehmigung durch die DSK zulässig sind. Die Genehmigungsfreiheit ergibt sich dabei grds wegen der in diesen Fällen generell anzunehmenden mangelnden Gefährdung von Betroffeneninteressen.[582]

Für die unternehmerische Praxis sind hierbei insb die Z 1 (die Daten sind bereits in Österreich veröffentlicht), Z 2 (die Daten sind lediglich indirekt personenbezogen), Z 5 (es liegt eine Zustimmung des Betroffenen vor), Z 6 (die Übermittlung ist zur Erfüllung eines Vertrages erforderlich) und Z 8 (die Übermittlung in den entsprechenden Drittstaat ist in einer StMV gelistet) relevant.[583]

Der Fall bereits veröffentlichter Daten wird iZm mit Due Diligence Prüfungen mE jedoch großteils unbeachtlich sein, da diese ja gerade darauf gerichtet sind, Informationen zu erlangen, die nicht ohne weiteres öffentlich zugänglich sind.

Ein indirekter Personenbezug wird sich dagegen in einer Vielzahl der Fälle eignen um Übermittlungen datenschutzkonform zu gestalten, nichtsdestotrotz kann in Einzelfällen die Einholung der Zustimmung einzelner Betroffener erforderlich sein.[584] Eine solche Zustimmung hat gem § 12 Abs 3 Z 5 ohne jeden Zweifel[585] zu erfolgen. Die hL geht davon aus, dass auch bei Übermittlungen in Drittstaaten eine konkludente Zustimmung möglich ist, doch müsse in diesem Fall eine strengerer Maßstab angelegt werden.[586] Konkludente Zustimmungen die entsprechend eindeutig sind, sind wohl am ehesten bei

---

[581] Dazu krit *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 12 Anm 2.
[582] *Flendrovsky/König/Kotschy*, Datenschutz – Teil I: Datenschutzkommission (DSK) in *Sachs/Thanner* (Hrsg), Verfahren vor Sonderbehörden (2006) 20.
[583] S *Knyrim*, Datenschutzrecht (2003) 128.
[584] Vgl zu dieser grds Konstellation schon Kap V.E.6.b)(2).
[585] Vgl dazu Art 26 Abs 1 lit a RL 95/46/EG.
[586] *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 12 Anm 14; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 156; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 285; auf letztere Bezug nehmend *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 59; krit dagegen *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 206.

einer Notwendigkeit der Übermittlung zur Vetragserfüllung denkbar; dafür besteht jedoch ohnehin eine eigene Ausnahme (zu dieser gleich).[587]

Zur Rechtfertigung zwecks Vertragserfüllung ist auf die Formulierung in § 12 Abs 3 Z 6 DSG, wonach der Vertrag eindeutig im Interesse des Betroffenen abgeschlossen worden sein muss, hinzuweisen.

Diese wird im interessierenden Fall uU zumindest eine etwas weitere Interpretation der Bestimmung erforderlich machen können. Der Vertrag zur Verfügungstellung personenbezogener Daten im Rahmen einer Due Diligence Prüfung wird nämlich zwischen der Zielgesellschaft und dem Akquisitionsinteressen abgeschlossen werden (so dass etwa mit den einzelnen Mitarbeitern des Zielunternehmens im Hinblick auf diese Übermittlung iE überhaupt kein Vertrag bestehen wird).

Dennoch wird man den Vertrag zur Due Diligence im Gros der Fälle mE als im Unternehmenswohl gelegen und somit zumeist auch im Interesse der Mitarbeiter beurteilen können. Ebenso wird man daher an das Kriterium, dass der Vertrag eindeutig im Interesse des datenschutzrechtlich Betroffen zu sein hat, keinen allzu strengen Maßstab anlegen dürfen, will man diesen Rechtfertigungsgrund nicht a priori als untauglich betrachten müssen.

Als weitere Ausnahme von der Genehmigungspflicht kommt schließlich die Auflistung von Drittstaaten in einer StMV in Betracht. Hierbei ist jedoch anzumerken, dass es für Übermittlungen im Rahmen von Due Diligence Prüfungen keine eigene(n) StMV gibt, weshalb sich umzustrukturierende Unternehmen auf diesen Rechtsfertigungsgrund iE nicht berufen können.[588]

b) Voraussetzungen der Zulässigkeit einer Übermittlung in Drittstaaten

Die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, an einen Empfänger in einem Drittland ist grds nur dann zulässig, wenn dieses Drittland ein angemessenes

[587] IdS auch *Knyrim*, Datenschutzrecht (2003) 129.
[588] S StMV 2004; vgl dazu auch *Trybus/Uitz*, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen? MR 2007, 346.

Schutzniveau gewährleistet.[589] In Einzelfällen können jedoch auch Übermittlungen in Drittländer ohne angemessenes Schutzniveau zulässig sein (dazu mehr in Kap V.F.3.c)).

Ob ein Drittstaat ein solcherart angemessenes Schutzniveau aufweist oder nicht entscheidet die EK mit bindender Wirkung für die Mitgliedstaaten.[590]

(1) Drittländer mit angemessenem Datenschutzniveau

Bislang wurde die Angemessenheit des Schutzniveaus für folgende Drittländer durch E der EK bindend anerkannt: Schweiz[591], Ungarn[592] (gleichwohl seit 1.5.2004 EU-Mitgliedstaat), Kanada[593], Jersey[594], Guernsey[595], Insel Man[596] und Argentinien[597].

Hinsichtlich der Schweiz und Ungarns erfolgte bereits 1999 durch eine V[598] iSd § 12 Abs 2 DSG eine Gleichstellung dieser Länder mit den EU-Mitgliedstaaten. Für die restlichen aufgezählten Drittländern existiert jedoch keine derartige V. Dies führt bei Umstrukturierungen in Zuge derer Daten in diese Länder übermittelt werden (etwa weil sich die Zielgesellschaft, ein Akquisitionsinteressent oder auch ein Datenraum Dienstleister dort befinden) zum unangenehmen Ergebnis, dass sich die Unternehmen jedes mal mit der Genehmigungspflicht des § 13 DSG konfrontiert sehen.

Ein Umstand der mE als äußerst unbefriedigend zu beurteilen ist, da entsprechende Genehmigungsverfahren aufgrund des damit verbundenen Aufwandes stets zeitliche Verzögerungen im Akquisitionsablauf verursachen werden. Diese stehen im

---

[589] Art 25 Abs 6 RL 95/46/EG.
[590] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 275.
[591] E der Kommission vom 26.7.2000 gem der RL 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl L 2000/215, 1.
[592] E der Kommission vom 26.7.2000 gem der RL 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl L 2000/215, 4.
[593] E der Kommission vom 20.12.2001 gem der RL 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl L 2002/2, 13.
[594] E der Kommission vom 8.5.2008 gem der RL 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Jersey, ABl L 2008/138, 21.
[595] E der Kommission vom 21.11.2003 über die Angemessenheit des Schutzes personenbezogener Daten in Guernsey, ABl L 2003/308, 27.
[596] E der Kommission vom 28.4.2004 über die Angemessenheit des Schutzes personenbezogener Daten auf der Insel Man, ABl L 2004/151, 51.
[597] E der Kommission vom 30.6.2003 über die Angemessenheit des Datenschutzniveaus in Argentinien, ABl L 2003/168, 19.
[598] Verordnung des Bundeskanzlers über den angemessen Datenschutz in Drittstaaten (Datenschutzangemessenheitsverordnung – DASV) BGBl II 1999/521.

Widerspruch zum generellen Interesse an einer raschen und rechtssicheren Durchführung der Due Diligence Prüfung. Schließlich werden im Rahmen dieser zahlreiche Unternehmensinterna offengelegt. Die im wirtschaftlichen Wettbewerb stehenden Betroffenen werden dabei aus nachvollziehbaren Gründen wenig Interesse daran haben, dass sich diese Daten, die für sie von vitalem Interesse sind, für längere Zeit quasi „freischwebend" in einem Genehmigungsverfahren befinden.

Eine Erlassung der noch ausstehenden V ist daher sowohl aus Sicht der einzelnen Betroffen als auch im Hinblick auf die wirtschaftliche Bedeutung einer sicheren Rechtsgrundlage angebracht.

(2) Sonderfall Übermittlung in die USA – das Safe Harbor Abkommen

Der Transfer personenbezogener Daten zwischen der EU und den USA ist aufgrund der zahlreichen Wirtschaftsbeziehungen zwischen diesen von besonders großer Bedeutung. Da das Verständnis datenschutzrechtlicher Sachverhalte in den USA ein grds anderes als in Europa ist[599], wurde schließlich ein eigenes Abkommen zum Schutz personenbezogener Daten geschlossen – das sog Safe Harbor Abkommen.[600]

Safe Harbor stellt sich dabei als ein komplexes Gebilde von sehr verschiedenen Dokumenten dar. Ausgangspunkt sind sechs vom US-Handelsministerium bzw von obersten Bundesbehörden im Zuge der Verhandlungen mit der EK übermittelte Grundlagenpapiere und Stellungnahmen. Innerhalb dieser Dokumente bilden erstens die Entscheidung der EK zur Anerkennung unternehmensbezogener Angemessenheit sowie zweitens deren Anlagen I (Grundsätze des sicheren Hafens) und II (Häufig gestellte Fragen – FAQ) den Kern des Abkommens.[601]

Danach haben amerikanische Unternehmen die Möglichkeit sich zur Einhaltung bestimmter datenschutzrechtlicher Bestimmungen (die weitestgehend den Anforderungen der diesbezüglichen europarechtlichen Regelungen entsprechen) zu

[599] S dazu Kap IV.C.
[600] E der Kommission vom 26.7.2000 gem der RL 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglich „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl L 2000/215, 7.
[601] *Genz*, Datenschutz in Europa und den USA (2004) 130.

verpflichten, um sich so zum „sicheren Hafen“ zu erklären, an den Datenübermittler aus der EU ihre Daten ohne weiteres übermitteln können.[602]

Das US-Handelsministerium führt ein öffentlich einsehbares Register, in dem die teilnehmenden Unternehmen (online) ersichtlich sind.[603] Die Registrierung für diese Liste wird jeweils für den Zeitraum von einem Jahr aufrechterhalten, danach ist eine neuerliche Registrierung bzw Bestätigung derselben erforderlich.[604]

Eine weitere Möglichkeit der Qualifikation ist die Teilnahme an einem Datenschutz- bzw Gütesiegelprogramm, das sich wiederum selbst den Safe Harbor Bestimmungen unterworfen hat. Als Bsp solcher Selbstregulierungsprogramme sind etwa TRUSTe[605] und BBBOnLine[606] zu nennen. Diese stellen Privacy Policies auf zu deren Einhaltung sich die Lizenznehmer des Gütesiegels verpflichten müssen. Hält ein Datenverarbeiter die vom Anbieter des Gütesiegels aufgestellten Datenschutzbestimmungen ein und entsprechen diese auch den Vorgaben des Safe Harbor Abkommens, hat sich der betreffende Datenverarbeiter grds für unbeschränkte Datentransfers aus der EU qualifiziert.[607] Zu erwähnen sind idZ auch die Bestrebungen zur Etablierung des europäischen Datenschutz-Gütesiegels („European Privacy Seal“, kurz „EuroPriSe“) als einem von der EU gefördertem Projekt, das die Ausstellung eines Europäischen Datenschutz-Gütesiegels für IT-Produkte und IT-Dienstleistungen bezweckt. Durch das Gütesiegel wird bestätigt, dass ein IT-Produkt oder eine IT-basierte Dienstleistung in Vereinbarkeit mit europäischem Datenschutzrecht eingesetzt werden kann.[608]

Auch im Hinblick auf das Safe Harbor Abkommen ist in Österreich bislang keine V gem § 12 Abs 2 DSG ergangen. Auch bei Datenübermittlungen in die USA haben Unternehmen daher – sofern kein materieller Ausnahmegrund iSd § 12 Abs 3 DSG vorliegt – stets einen Genehmigungsantrag an die DSK zu stellen. Auch hier ist die Erlassung einer entsprechenden V angezeigt, da sich die Konsequenzen dieser fehlenden Regelung ebenso wie im Verhältnis zu sonstigen Drittländern als wirtschaftliches Hemmnis darstellen.

---

[602] *Knyrim*, Datenschutzrecht (2003) 134.
[603] http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (6.3.2009).
[604] *Genz*, Datenschutz in Europa und den USA (2004) 132.
[605] http://www.truste.org/ (6.3.2009).
[606] http://www.bbb.org/online/ (6.3.2009).
[607] *Genz*, Datenschutz in Europa und den USA (2004) 133.
[608] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 14 Anm 21.

(3) Standardvertragsklauseln

Standvertragsklauseln sind ein Instrument nach Art 26 Abs 2 RL 95/46/EG um iE auch eine Übermittlung personenbezogener Daten in Drittländer, die prima facie über kein angemessenes Schutzniveau verfügen, zu ermöglichen.

Solche Übermittlungen sind zulässig, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet.[609] Die Übermittlung darf also nicht trotz Fehlens eines angemessenen Schutzniveaus erfolgen, sondern weil eben gerade für den konkreten Fall der Schutz garantiert ist.[610]

Das wichtigste Mittel um entsprechende Garantien zu begründen sind dabei vertragliche Vereinbarungen.[611] Art 26 Abs 4 RL 95/46/EG sieht vor, dass die EK befinden kann, dass bestimmte Standardvertragsklauseln ausreichende Garantien bieten können. Bis dato existieren zwei entsprechende Entscheidungen der EK: zum einen betreffend Datenübermittlungen in Drittländer[612] (wobei die bloße Überlassung an Dienstleister jedoch nicht erfasst ist), zum anderen betreffend „Übermittlungen" zur Überlassung an Dienstleister in Drittstaaten[613] (wobei hier wiederum ausdrücklich nur Überlassungen an Dienstleister erfasst sind). Die Diktion dieser sog Auftragsverarbeiter-Standardvertragsklausel der EK ist dabei im Lichte der Begrifflichkeiten des österr DSG leicht missverständlich. Derartige Übermittlungen werden in Österreich nämlich stets als Überlassungen iSd § 4 Z 11 DSG zu beurteilen sein.

Zur Umsetzung der Entscheidungen der EK in das österr Recht hat der Bundeskanzler die Möglichkeit trotz Fehlens eines im Empfängerstaat generell geltenden Schutzniveaus durch V festzustellen, dass für bestimmte Kategorien des Datenverkehrs

---

[609] Art 26 Abs 2 RL 95/46/EG.
[610] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 288.
[611] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar (1997) 289.
[612] E der Kommission vom 15.6.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der RL 95/46/EG, ABl L 2001/181, 19; E der Kommission vom 24.12.2004 zur Änderung der E 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl L 2004/385, 74.
[613] E der Kommission vom 27.12.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der RL 95/46/EG, ABl L 2002, 52.

mit diesem Empfängerstaat die Voraussetzungen nach § 13 Abs 2 Z 1 DSG (dh hier das Bestehen eines angemessenen Datenschutzes im konkreten Einzelfall) zutreffen.[614] Gem § 13 Abs 7 DSG tritt diesfalls an die Stelle der Verpflichtung zur Einholung der Genehmigung die Pflicht zur Anzeige an die DSK.[615]

Auch bezüglich der Komissionsentscheidungen betreffend Standardvertragsklauseln ist bislang keine Umsetzung durch V des Bundeskanzler erfolgt. Dh dass bei Umstrukturierungen in Zuge derer es zu Datenübermittlung in Drittländer kommt, wobei mit dem dortigen Empfänger (gleich, ob als datenschutzrechtlichem Auftraggeber oder Dienstleister) Standardvertragsklauseln unterfertigt wurden, eine ausdrückliche Antragsstellung an die DSK erforderlich ist. Wiederum besteht für Unternehmen in derartigen Fällen die Möglichkeit eines vereinfachten Anzeigeverfahrens nicht.

Ein Lösungsansatz für datenexportierende Auftraggeber könnte möglicherweise darin bestehen sich direkt auf die Entscheidungen der EK zu berufen.[616] In Anbetracht des derzeitigen status quo muss jedoch auch in diesem Fall die Untätigkeit des (materiellen) Gesetzgebers iE als Behinderung unternehmerischer Prozesse konstatiert werden.

c) Die Genehmigung durch die DSK

Liegt weder einer der materiellen Ausnahmegründe nach § 12 Abs 3 DSG vor, noch ist das Drittland (in dem sich der Empfänger der Daten befindet) der EU nach § 12 Abs 2 DSG gleichgestellt, noch möchten Datenexporteur und Datenimporteur Standardvertragsklauseln abschließen, muss die Übermittlung durch die DSK mittels individueller Prüfung im Einzelfall genehmigt werden.[617]

(1) Voraussetzungen einer Genehmigung

Die konkreten Voraussetzungen einer Genehmigung sind in § 13 Abs 2 DSG geregelt. Vor dem Hintergrund gesellschaftsrechtlicher Umstrukturierungen wird es das im

[614] § 55 Z 2 DSG.
[615] § 13 Abs 7 DSG; vgl dazu *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 161.
[616] IdS *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 13 Anm 12.
[617] ErläutRV 1613 BlgNR 20. GP 42; vgl dazu auch *Knyrim*, Datenschutzrecht (2003) 148.

Rahmen der Due Diligence geprüften und somit übermittelnden Unternehmen sein, das als datenschutzrechtlicher Auftraggeber zu beurteilen sein wird.
Diesem stehen iE zwei Möglichkeiten offen um eine Genehmigung der Datenübermittlung (bzw Datenüberlassung) zu erreichen: Zum einen kann die DSK feststellen, dass im konkreten Einzelfall ein angemessenes Datenschutzniveau besteht[618], zum anderen kann das Unternehmen glaubhaft machen, dass die schutzwürdigen Geheimhaltungsinteressen der Betroffenen auch im Empfängerstaat gewahrt sind.[619]

Bei der Feststellung eines angemessenen Schutzniveaus im Einzelfall stellt die DSK eine Gesamtbetrachtung der Umstände der Übermittlung an.[620] Ob nun konkret Angemessenheit vorliegt, bestimmt sich nach der Art (Sensibilität) der personenbezogenen Daten, dem Verwendungszweck und der Dauer der Verwendung. Des weiteren ist der Entwicklungsstand der Rechtsordnung (rechtsstaatliche Garantien, effektiver Rechtsschutz etc), bereichsspezifische Regelungen (wie etwa im Bankwesen) aber auch an sich nicht allgemein rechtsverbindliche Übereinkünfte, sog soft law (zB Standesregeln), zu berücksichtigen.[621]

Ist die derartige Feststellung eines angemessenen Schutzniveaus nicht möglich, muss das datenexportierende Unternehmen glaubhaft machen, dass die schutzwürdigen Geheimhaltungsinteressen auch im Drittland gewährleistet sind. Hierfür bieten sich insb vertragliche Vereinbarungen über datenschutzrechtliche Verpflichtungen des Empfängers an (wie die bereits oa Standardvetragsklauseln). Aber auch jede andere vertragliche Vereinbarung hinsichtlich des Datenschutzes in einem Vertrag kann der Glaubhaftmachung eines angemessenen Schutzniveaus und damit einer Genehmigung durch die DSK dienlich sein.[622]

(2) Das Genehmigungsverfahren

Sofern keine der oa Ausnahmen greift, bedürfen sowohl Übermittlungen als auch bloße Überlassungen in Drittländer der Genehmigung durch die DSK. Abweichend von

---

[618] § 13 Abs 2 Z 1 DSG.
[619] § 13 Abs 2 Z 2 DSG.
[620] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 161.
[621] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 13 Anm 7.
[622] *Knyrim*, Datenschutzrecht (2003) 150.

§ 13 Abs 1 DSG haben nicht nur der Auftraggeber sondern gem § 13 Abs 5 DSG auch inländische Dienstleister die Möglichkeit für ihre Kunden (dh Auftraggeber) Anträge zu stellen. Eine Bestimmung die iZm Due Diligence Prüfungen etwa für einen österr Datenraum Dienstleister von Bedeutung sein kann, idR jedoch eher EDV-Wartungsfirmen mit großer Kundenzahl betreffen wird.[623]

Da das Genehmigungsverfahren nur auf Antrag[624] eingeleitet wird, muss daher der Auftraggeber oder Dienstleister, der personenbezogene Daten in Drittländer übermitteln möchte, bei der DSK den entsprechenden Antrag stellen. Dieser Antrag ist formlos, jedoch sollten jedenfalls folgende Informationen gegeben werden: Bezeichnung des Antragstellers, Sitz und Bezeichnung des ausländischen Datenempfängers, die Angabe, ob es sich um eine Übermittlung oder Überlassung handeln soll, Zweck des Transfers, Darlegung der Rechtsgrundlage, Bezeichnung der Datenanwendung, aus der die Daten stammen, die exportiert werden sollen, Angaben über die Datenarten, die transferiert werden sollen sowie Darlegungen betreffend den ausreichenden Rechtsschutz beim Empfänger.[625]

Zwar ist der Antrag unabhängig von der grds Meldepflicht einer Datenverarbeitung beim DVR, für das umzustrukturierende Unternehmen wird sich jedoch bei komplexeren Verarbeitungen eine gemeinsame Einbringung der Anträge nach § 17 und § 13 DSG empfehlen.[626] Hinzuweisen ist idZ auch auf den Umstand, dass eine unterlassene Genehmigung der Übermittlung in Drittländer eine Verwaltungsstrafe von bis zu € 9.445,-- nach sich ziehen kann.[627]

Beim vereinfachten Anzeigeverfahren nach § 13 Abs 7 DSG hat die DSK binnen sechs Wochen den angezeigten Datenverkehr zu untersagen, andernfalls ist die Übermittlung oder Überlassung der Daten in das Drittland zulässig. Wie bereits mehrfach dargestellt ist dieses Anzeigeverfahren jedoch mangels österr Rechtsgrundlagen in vielen Fällen nicht möglich. Dies bedeutet iE, dass für das Genehmigungsverfahren vor der DSK nicht einmal eine Entscheidungspflicht von sechs Wochen angenommen werden kann.

---

[623] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 13 Anm 11.
[624] Arg der Formulierung in § 13 Abs 1 erster S DSG.
[625] *Flendrovsky/König/Kotschy*, Datenschutz – Teil I: Datenschutzkommission (DSK) in *Sachs/Thanner* (Hrsg), Verfahren vor Sonderbehörden (2006) 24.
[626] IdS auch *Knyrim*, Datenschutzrecht (2003) 151.
[627] § 52 Abs 2 Z 2 DSG; s Kap IV.B.3.

Zwar ist eine sorgfältige und genaue Prüfung des Datenverkehrs mit Sicherheit wünschenswert, die daraus zT resultierenden langfristigen Verfahren sind jedoch keinesfalls im Interesse der an einer Akquisition beteiligten Unternehmen.

Zusammenfassend muss jedenfalls konstatiert werden, dass sich für Unternehmen in Umstrukturierungsprozessen (gerade iZm Übermittlungen in Drittländer) die derzeitige Rechtslage als iE unbefriedigend darstellt. Aufgrund der mangelnden Umsetzung europäischer E betreffend jene Drittländer, für die ein angemessenes Datenschutzniveau bereits verbindlich festgestellt wurde, ist im jeweiligen Einzelfall nach wie vor ein zeitraubendes Genehmigungsverfahren zu durchlaufen. Dieser Umstand steht im Widerspruch zu den wirtschaftlichen Interessen aller an einer Unternehmensakquisition Beteiligten selbige möglichst rasch und rechtssicher abwickeln zu können. Die Erlassung entsprechender nationaler Regelungen ist mE somit angezeigt; dies nicht zuletzt im Interesse der Qualität des österr Wirtschaftsstandortes.

VI. Datenschutzrechtliche Fragestellungen im Konzern

Abgesehen von Datenflüssen im Zuge gesellschaftsrechtlicher Umstrukturierungen kommt es auch innerhalb von Unternehmen regelmäßig zu einer Verarbeitung und insb Übermittlung personenbezogener Daten. Gerade bei Konzernstrukturen ist ein reger Datenverkehr zu beobachten.[628] Unter einem Konzern ist gem § 15 AktG eine Zusammenfassung von rechtlich selbständigen Unternehmen zu wirtschaftlichen Zwecken unter einheitlicher Leitung oder Beherrschung zu verstehen.

Dabei ist zum einen an den im unternehmerischen Alltag üblichen und notwendigen Datenaustausch zwischen den einzelnen Organisationseinheiten des Unternehmens zu denken, zum anderen auch an solche Informationsflüsse die nicht innerhalb der herkömmlichen Unternehmensstrukturen ablaufen. Letzteres kann va im Rahmen unternehmensinterner Kontrollsysteme stattfinden (auch sog Whistleblowing, dazu gleich mehr).[629]

Der ao Informationsaustausch findet insb im Rahmen sog Informationsverbundsysteme statt, den Untersuchungen einzelner Übermittlungstatbestände wird daher ein kurzes Kap zur datenschutzrechtlichen Charakteristik dieser Systeme vorangestellt.

A. Informationsverbundsysteme im Konzern – begrifflicher Inhalt und Voraussetzungen

Gem der Legaldefinition des § 4 Z 13 DSG ist ein Informationsverbundsystem die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden. Für das Vorliegen eines Informationsverbundsystems ist iE daher Voraussetzung dass erstens Daten in einer

---

[628] *Knyrim*, Datenschutz bremst Austausch in internationalen Konzernen, Die Presse vom 30.10.2006; ders Einspielung österreichischer Kunden- und Mitarbeiterdaten in internationale Konzerndatenbanken: Vorsicht! Die Presse vom 31.5.2003.

[629] *Spring*, „Whistleblowing" – „Verpfeif"-Maßnahmen aus datenschutzrechtlicher Sicht, ecolex 2007, 139.

Datenanwendung durch mehrere Auftraggeber verarbeitet werden und zweitens jeder auf die Daten des jeweils anderen im System Zugriff hat.[630]

Für Unternehmen die sich solcher Systeme bedienen sind nun zahlreiche datenschutzrechtliche Erfordernisse zu beachten: Das DSG unterwirft Informationsverbundsysteme der Vorabkontrolle durch die DSK[631] und fordert weiters für deren Zulässigkeit die Bestellung eines Betreibers[632], der sowohl für die Wahrnehmung der Betroffenenrechte als auch für die Datensicherheit verantwortlich ist.[633]

Des weiteren trifft den Betreiber die Pflicht, jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen.[634] Die oa Meldepflichten können für Unternehmen einen nicht unerheblichen organisatorischen Aufwand bedeuten weshalb bereits bei Implementierung eines Informationsverbundsystems eine Vorausplanung der Abwicklung etwaiger Auskunftsbegehren anzuraten sein wird.

Im Anschluss werden nun exemplarisch zwei für den konzerninternen Datenverkehr typische Sachverhalte und deren datenschutzrechtlicher Gehalt untersucht.

B. Fälle des Datenflusses zwischen den einzelnen Organisationseinheiten des Konzerns

Vorerst ist nochmals das Wesen Datenübermittlung kurz darzustellen, da deren Begriffskern im gegenständlichen Bereich eminente Bedeutung zukommt. Eine Übermittlung personenbezogener Daten kann demnach in drei Formen auftreten: Erstens als Weitergabe an einen Dritten (ein anderer Empfänger als Betroffener,

---

[630] IglS *Knyrim*, Datenschutzrecht (2003) 21; vgl dazu auch *Oberndorfer/Trybus*, Die (un)überwindbaren Schranken des Datenschutzrechts für Unternehmen mit Fokus auf Informationsverbundsysteme, in *Schweighofer/Geist/Heindl* (Hrsg), 10 Jahre Iris: Bilanz und Ausblick, IRIS 2007, 301.
[631] § 18 Abs 2 Z 4 DSG.
[632] § 50 Abs 1 DSG.
[633] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 4 Anm 14.
[634] § 50 Abs 1 DS.

Auftraggeber oder Dienstleister)[635], zweitens als Veröffentlichung und drittens als Verwendung für ein anderes Aufgabengebiet desselben Auftraggebers.[636]

1. Übermittlung durch Wechsel des datenschutzrechtlichen Aufgabengebietes im Konzern

Im Konzern kann va eine Datenverwendung für unterschiedliche Aufgabengebiete des Auftraggebers als Übermittlungsform auftreten. Soweit ein Aufgabengebiet dabei nicht gesetzlich vorgeschrieben ist, ist es nach dem vom Auftraggeber mit der Datenverarbeitung verfolgten Zweck zu bestimmen.[637] Im privaten Bereich soll das Aufgabengebiet in etwa mit dem Umfang einer Gewerbeberechtigung gleichzusetzen sein.[638]

Die Abgrenzung des Aufgabengebietes ist in der Lit und Rsp jedenfalls nicht einheitlich; so sollen zur Vermeidung einer praxisfernen Auslegung auch mehrere Gewerbeberechtigungen als ein Aufgabengebiet zu verstehen sein[639], zum anderen besteht eine Jud des OGH, wonach die Führung von Girokonten und der Abschluss von Bausparverträgen jeweils verschiedene Aufgabengebiete eines Auftraggebers seien.[640] In letzterem Fall wäre zumindest argumentierbar, dass beide Tätigkeiten in das übliche Geschäftsfeld einer Bank fallen.

In Anbetracht der enormen Vielfalt von Datenverwendungen in der Privatwirtschaft wird sich meiner Auffassung nach iE eine Beurteilung des Inhaltes eines Aufgabengebietes nach der in den jeweiligen Geschäftskreisen herrschenden Verkehrsauffassung als sachgerecht erweisen können.[641]

Bei einem Informationsaustausch zwischen den einzelnen Unternehmen in einem Konzern ist somit auch darauf Bedacht zu nehmen, dass dadurch auch datenschutzrechtlich relevante Übermittlungen „in sich“ stattfinden können, bei denen die Zulässigkeit geprüft werden muss. Gerade bei der Erweiterung von Geschäftsfeldern

---

[635] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 4 Anm 13.
[636] Vgl *Knyrim*, Datenschutzrecht (2003) 115.
[637] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 123.
[638] ErläutRV 1613 BlgNR 20. GP 39.
[639] IdS *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 4 Anm 13.
[640] OGH 25.2.1992, 4 Ob 114/91.
[641] IglS *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 4 Anm 13.

im Rahmen von Unternehmensumstrukturierungen (etwa durch Verschmelzungen) können sich derartige Sachverhalte ergeben.[642]

Werden bspw in einem einzelnen Unternehmen ermittelte Kundendaten außerhalb ihres ursprünglichen Zweckes auch in anderen Konzernunternehmen verwendet (etwa um dann Rückschlüsse für eine konzernweite Geschäftspolitik zu gewinnen) kann dies uU bereits als Übermittlung zu betrachten sein.

2. Übermittlungen im Rahmen von Standardanwendungen – spezifische Problemfälle

Als unternehmensinterner Bereich in dem es regelmäßig zur Übermittlung personenbezogener Daten kommen wird, ist va die Personalverwaltung zu nennen. Problematisch idZ ist, dass zwar eine Standardanwendung „Personalverwaltung für privatrechtliche Dienstverhältnisse“[643] existiert, diese jedoch überhaupt keine Übermittlungen im Konzern vorsieht. Dies bedeutet iE, dass eine Übermittlung von Personaldaten im Konzern zumindest beim DVR anzuzeigen (solange sich der Konzern auf EU-Mitgliedstaaten beschränkt) ist, zT jedoch sogar der Genehmigungspflicht durch die DSK unterliegen kann (sofern die Konzernstruktur auch Drittländer umfasst).

Aber auch im Hinblick auf Kundendaten können sich datenschutzrechtliche Implikationen ergeben. Gem der Standardanwendung „Rechnungswesen und Logistik“[644] sind Übermittlungen an die Konzernleitung eines Auftraggebers bei Lieferanten sowie an gewerbliche Kunden und Großkunden (dh die Leistungsempfänger) auch dann zulässig, wenn sich diese in einem Drittland befinden. Nicht zulässig sind jedoch Übermittlungen an andere Unternehmen bzw Gesellschaften (sog Schwestergesellschaften) des Konzerns. Sowie im Rahmen der Personalverwaltung können daher im Anlassfall Registrierungen bzw auch langfristige Genehmigungsverfahren zu durchlaufen sein.

---

[642] *Knyrim*, Datenschutzrecht (2003) 118.
[643] SA002; s Anlage 1 StMV 2004.
[644] SA001; s Anlage 1 StMV 2004.

Hinzu kommt weiters, dass eine privilegierte Übermittlung in Drittländer nur für gewerbliche Kunden besteht, nichtgewerbliche Kunden und „Kleinkunden“[645] sind dagegen nicht erfasst. Unternehmen, deren Kunden Endverbraucher sind, müssen entsprechende Übermittlungen daher jedenfalls beim DVR melden.[646]

3. Übermittlungen durch Kontrollsysteme im Konzern am Beispiel des Us-amerikanischen Whistleblowing

In den letzten Jahren haben sich, ausgehend vom amerikanischen Raum, in zahlreichen Unternehmen Kontrollsysteme etabliert, die mit dem Schlagwort des „Whistleblowing“ bezeichnet werden. Für diesen Begriff existieren mehrere Definitionen, eine in der Lit gängige lautet: „Die Enthüllung illegaler, unmoralischer oder illegitimer Verhaltensweisen durch einem Arbeitgeber unterstehende (gegenwärtige oder ehemalige) Mitarbeiter, gegenüber einer Person oder Organisation, die die Möglichkeit besitzt, das Vorgehen zu beeinflussen.“[647]

Ausgehend vom Zusammenbruch der amerikanischen Unternehmen Enron und Worldcom (bei denen eben durch ein der oa Vorgehensweise entsprechendes Verhalten milliardenschwere Bilanzfälschungen aufgedeckt wurden)[648] beschloss der US-Kongress den „Sarbanes-Oxley Act“.[649] Telos dieser Regelung ist die Erhöhung der Anforderungen an die Finanzberichterstattung sowie eine Steigerung der Wirksamkeit interner Kontrollen. IZm Konzernstrukturen ist va der Umstand relevant, dass alle Unternehmen, deren Aktien in den USA gehandelt werden, die Bestimmungen des SOX anzuwenden haben. Dies bedeutet iE, dass österr Unternehmen den SOX anzuwenden haben, soweit sie oder ihre amerikanische Muttergesellschaft an einer US-Börse notieren.[650]

---

[645] Darunter sind va Konsumenten zu verstehen.
[646] *Knyrim*, Datenschutzrecht (2003) 38.
[647] MwN *Kittelberger*, External Reporting als Pflicht zum Whistleblowing? ÖBA 2007, 92; zur Übersetzung aus dem Englischen vgl *Lehner*, Whistleblowing-Hotlines gemäß SOX in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 151.
[648] *Berndt/Hoppler*, Whistleblowing – Ein integraler Bestandteil effektiver Corporate Governance, BB 2005, 2626; vgl dazu auch *Knyrim/Kurz/Haidinger*, Whistleblowing-Hotlines: Mitarbeiter „verpfeifen“ zulässig? ARD 2006 Heft 5681, 3.
[649] Sarbanes-Oxley Act 2002, s http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley (16.3.2002).
[650] *Spring*, “Whistleblowing“ – „Verpfeif“-Maßnahmen aus datenschutzrechtlicher Sicht, ecolex 2007, 139; für D vgl *Wisskirchen/Körber/Bissels*, „Whistleblowing“ und „Ethikhotlines“, BB 2006, 1567.

Aus datenschutzrechtlicher Sicht interessiert insb die Bestimmung Sect 301 P 4 SOX; dieser zufolge ist ein Verfahren zur Abwicklung von übermittelten Meldungen bezüglich fraglicher Buchführungs- und Bilanzierungspraktiken einzuführen. Eine konkrete Einrichtung telefonischer Hotlines ist zwar nicht gefordert, dennoch haben viele amerikanische Unternehmen solche im Rahmen interner Unternehmensrichtlinien[651] vorgesehen.

Im Rahmen von Whistleblowing-Systemen werden regelmäßig Informationen über in Verdacht geratene Personen weitergegeben; zu denken ist bspw an deren Name, die Abteilung sowie das etwaige Fehlverhalten. Dies ist unzweifelhaft notwendig, da andernfalls ein Kontrollsystem seinen Zweck nur schwerlich erfüllen wird können. Da diese Daten jedoch personenbezogen iSd § 4 Z 1 DSG sind, liegt in weiterer Folge auch ein Verwenden personenbezogener Daten iSd § 4 Z 8 DSG vor; Konsequenz dessen ist die datenschutzrechtliche Beachtlichkeit derartiger Vorgänge.

a) Allgemeine Voraussetzungen für die datenschutzrechtliche Zulässigkeit eines Whistleblowing-Systems nach SOX

Damit ein (telefonisches) Verfahren zur Meldung von Missständen legitim ist, muss die Einrichtung eines solchen entweder für die Erfüllung einer rechtlichen Verpflichtung[652] (der der für die Datenverarbeitung Verantwortliche unterliegt) erforderlich sein oder es muss für die Verwirklichung der berechtigten Interessen[653] des für die Datenverarbeitung Verantwortlichen notwendig sein.[654] Für europäische Konzernunternehmen kann der SOX als ausländisches Recht dabei keine rechtliche Verpflichtung iSd der RL 95/46/EG darstellen. Andernfalls bestünde die Gefahr einer Umgehung der europarechtlichen Vorschriften zum Datenschutz.[655]

---

[651] Sog „Code of Conduct".
[652] Art 7 lit c RL 95/46/EG.
[653] Art 7 lit f RL 95/46/EG.
[654] Vgl dazu *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen, Rechnungslegung, Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken und Finanzkriminalität, 8; abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf (16.3.2009).
[655] IglS *Lehner*, Whistleblowing-Hotlines gemäß SOX in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 165; *Knyrim/Kurz/Haidinger*, Whistleblowing-Hotlines: Mitarbeiter „verpfeifen" zulässig? ARD 2006 Heft 5681, 5.

Da das österr DSG bis dato keine derartigen Kontrollsysteme vorsieht, ist die bekannte Interessensabwägung vorzunehmen um iE zu einer Zulässigkeit von Whistleblowing-Hotlines zu kommen.[656] Eine solche dürfte idR zugunsten des Unternehmens ausfallen, insb erkennt die Art 29 Datenschutzgruppe grds die Bedeutung der Einhaltung von guten Grundsätzen der Unternehmensführung an.[657] Die Einführung eines Kontrollsystems nach SOX wird sich mE für österr Unternehmen daher gem § 8 Abs 1 Z 4 DSG rechtfertigen lassen.

Nichtsdestotrotz sind bei Implementierung derartiger Kontroll- und Meldeverfahren stets auch die allgemeinen Grundsätze jeder Datenverwendung zu beachten.[658] IZm mit Whistleblowing-Hotlines kann sich dabei va das Erfordernis einer Datenverwendung nach Treu und Glauben als problematisch erweisen. Eine solche liegt nur vor, wenn der Betroffene über die Umstände des Datengebrauchs und das Bestehen sowie die Durchsetzbarkeit seiner Rechte nicht irregeführt oder im Unklaren gelassen wird.[659]

So wird sich wohl insb eine entsprechende Information des Unternehmens gegenüber den Mitarbeitern iSd § 24 Abs 2 DSG als Zulässigkeitsvoraussetzung darstellen.[660] Insofern wird der von der Whistleblowing-Hotline erfasste Personenkreis über die Existenz, den Zweck und die Funktionsweise des Systems, die Empfänger der Meldungen sowie die Zugangs-, Auskunfts- und Berichtigungsrechte seiner Daten zu informieren sein.[661] Des Weiteren ist dem Verdächtigen die Identität des für die Datenverwendung im Rahmen des Whistleblowing-Systems verantwortlichen Auftraggebers bekanntzugeben.

In einem besonderen Spannungsverhältnis zum Grundsatz von Treu und Glauben steht der Umstand, dass der SOX an sich ein anonymes Meldeverfahren vorsieht. Insb die Art 29 Datenschutzgruppe kritisiert diese mangelnde Identifizierbarkeit des Hinweisgebers.[662] Dies könnte jedoch iE die Hemmschwelle der Mitarbeiter zur Meldung potentieller Missstände extrem erhöhen, was wiederum die Effizienz des

---

[656] IdS auch *Dohr/Pollirer/Weiss*, DSG[2] (2002) Anh V/17, 418.
[657] *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 9.
[658] § 6 DSG; vgl dazu *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 10.
[659] ErläutRV 1613 BlgNR 20. GP 39.
[660] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 24 Anm 3; *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 24 Anm 7.
[661] *Lehner*, Whistleblowing-Hotlines gemäß SOX in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 173; vgl *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 14.
[662] *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 11 (12).

Kontrollsystems deutlich mindern würde. Eine mögliche Lösung dieses Problems kann in einer Abwicklung des Meldeverfahrens durch externe Dienstleister bestehen.[663] Dadurch bestünde die Möglichkeit eines anonymen Meldeverfahrens, ein Zugriff auf Insiderwissen sowie gleichzeitig auch eine Rückfragemöglichkeit. Im Zuge einer Gesamtschau der bezüglich der Identifizierbarkeit des Hinweisgebers vorgebrachten Argumente wird sich ein Auslagern des Meldeverfahrens an entsprechend spezialisierte Unternehmen[664] meiner Auffassung nach als durchaus sachgerecht erweisen können.

b) Whistleblowing-Systeme in multinationalen Konzernen – besondere datenschutzrechtliche Anforderungen

Besondere Fragen stellen sich nun bei einer Konzernstruktur von multinational tätigen Unternehmen. Grds ist die Bearbeitung der Meldungen stets in der lokalen Organisation (diesfalls in einem Unternehmen innerhalb des europäischen Binnenmarktes) vorzunehmen. Jedoch bestehen in der Praxis oft konzernweite Berichtspflichten für EU-Tochtergesellschaften an ihre Muttergesellschaften, die wiederum ihren Sitz meist in Drittländern haben.[665] Für den Fall, dass das betreffende Drittland kein angemessenes Schutzniveau aufweist ist die Übermittlung gem der Art 29 Datenschutzgruppe unter folgenden Voraussetzungen zulässig:[666]

1. Der Empfänger der personenbezogenen Daten ist eine in den USA niedergelassene Einheit, die die Grundsätze des Safe Harbor Abkommen angenommen hat.
2. der Empfänger hat mit dem EU-Unternehmen, das die Daten übermittelt, einen Übermittlungsvertrag abgeschlossen und dieser Vertrag sieht ausreichende Garantien zum Datenschutz vor;[667]

---

[663] IdS auch *Lehner*, Whistleblowing-Hotlines gemäß SOX in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 171.

[664] Als solche Unternehmen kommen etwa Call Center oder auch Anwaltskanzleien in Betracht; vgl dazu *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 18.

[665] Zu den einzelnen datenschutzrechtlichen Fragestellungen iZm Übermittlungen in Drittländer s Kap V.F.

[666] *Art 29 Datenschutzgruppe*, Stellungnahme 1/2006, 19.

[667] Explizit in der Stellungnahme der Art 29 Datenschutzgruppe angeführt sind die E der Kommission vom 15.6.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der RL 95/46/EG, ABl L 2001/181, 19 sowie die E der Kommission vom 24.12.2004 zur Änderung der E 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl L 2004/385, 74.

3. der Empfänger hat verbindliche Unternehmensregelungen eingeführt, die von den zuständigen Datenschutzstellen genehmigt wurden.[668]

Unabhängig von der Zulässigkeit der Datenerhebung und –verarbeitung mittels einer Whistleblowing-Hotline ist somit auch zu prüfen, ob ein berechtigtes Interesse für die Übermittlung der gewonnen Daten vorliegt. Ist dies zu bejahen, sind die Vorschriften des DSG hinsichtlich einer allfälligen Genehmigung durch die DSK zu beachten.[669]

Schließlich ist auch noch darauf hinzuweisen, dass Meldungen im Rahmen oa Kontrollsysteme im Gros der Fälle ein strafrechtlich relevantes Verhalten betreffen werden. Strafrechtlich relevante Daten dürfen gem § 8 Abs 4 Z 3 DSG nur bei Vorliegen gesetzlicher Sorgfaltspflichten oder bei einem überwiegendem berechtigten Interesse des Auftraggebers verwendet werden. Wie bereits dargelegt, wird sich die Einführung einer Whistleblowing-Hotline meist über eine Interessensabwägung rechtfertigen lassen; damit ist mE auch schon das gewichtigste Argument für die Zulässigkeit dieses Meldeverfahrens gegeben, verfolgt dieses ja doch gerade den Zweck rechtswidriges Verhalten aufzudecken.

Whistleblowing-Systeme sind somit mit den Anforderungen des DSG (bzw dessen europarechtlichen Vorgaben) durchaus nicht unvereinbar. Wie gezeigt wurde, sind jedoch zahlreiche datenschutzrechtliche Vorgaben zu beachten, insb bietet die Stellungnahme der Art 29 Datenschutzgruppe eine entsprechende Orientierung. Letzteres, da das DSG bis dato keinerlei Regelungen zu derartigen Kontrollsystemen enthält. [670]

Zusammenfassend muss für diesen Bereich der Verwendung personenbezogener Daten, eine nicht unerhebliche Rechtsunsicherheit für Unternehmen konstatiert werden. Dies

---

[668] Sog Binding Corporate Rules; vgl *Knyrim/Kurz/Haidinger*, Whistleblowing-Hotlines: Mitarbeiter „verpfeifen" zulässig? ARD 2006 Heft 5681, 6.

[669] *Lehner*, Whistleblowing-Hotlines gemäß SOX in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 177.

[670] Hinzuweisen ist idZ jedoch auf eine jüngst ergangene E der DSK betreffend die Implementierung eines Whistleblowing-Systems: E DSK 5.12.2008, K178.274/0010-DSK/2008; s dazu die Kritik der *ARGE Daten*, DSK genehmigt Weitergabe von „whistle blowing"-Daten in die USA http://www2.argedaten.at/session/anonym238665oatzzx650535.E42_INP.html (21.3.2009); vgl *Leissler*, „Whistleblowing" in Österreich, die ersten Schritte…, ecolex 2009, 361; krit auch *Graf/Riesenhuber*, Whistleblowing-Hotline: Bescheid der DSK zu GZ K178.274/0010-DSK/2008 vom 5.12.2008 – Einige gelöste, viele offene Fragen, jusIT 2009, 143.

insb, da zu erwarten ist, dass die datenschutzrechtlichen Fragestellungen iZm konzernweiten Kontrollsystem an Bedeutung weiter zunehmen werden.

VII. Datenschutz und IT-Sicherheit im Unternehmen

Auch in Bezug auf die unternehmensinterne Organisation kommt dem Datenschutz, insb unter dem Aspekt der IT-Sicherheit, große Bedeutung zu. Der richtige Umgang mit IT entscheidet nicht selten darüber, ob ein Unternehmen am Markt reüssieren kann oder nicht. Mängel beim Datenschutz und der IT-Sicherheit können die Existenz des Unternehmens bedrohen. Nicht zuletzt kann die Gewährleistung einer datenschutzkonformen Organisation auch zum Inhalt der unternehmerischen Sorgfaltspflicht werden.[671] Im Folgenden wird ein Überblick über jene sicherheitsrelevanten Bereiche des Unternehmens geboten, die idR datenschutzrechtliche Implikationen nach sich ziehen können.

A. Maßnahmen zur Datensicherheit

Auftraggeber oder Dienstleister, die Daten verwenden, sind gem § 14 DSG dazu verpflichtet Datensicherheitsmaßnahmen zu ergreifen. Nach Abs 1 der Bestimmung müssen sie für alle ihre Organisationseinheiten Maßnahmen zur Gewährleistung der Datensicherheit treffen. Je nach Art der verwendeten Daten, dem Umfang und Zweck der Verwendung und unter Bedachtnahme auf den Stand der technischen Möglichkeiten sowie die wirtschaftliche Vertretbarkeit müssen Vorkehrungen getroffen werden, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind; weiters, dass die Verwendung der Daten ordnungsgemäß erfolgt und dass diese Daten Unbefugten nicht zur Kenntnis gelangen.[672]

1. Grundlagen einer datenschutzkonformen Organisation

In der angewandten Informatik umfasst der Begriff Datensicherheit drei Komponenten, und zwar Vertraulichkeit (Datenzugriff nur durch befugte Personen), Integrität (die verwendeten Daten haben richtig, vollständig und aktuell zu sein) sowie Verfügbarkeit (so müssen die entsprechenden IT-Systeme für die Benützer verfügbar sein).[673]

---

[671] IdS *Hasberger*, IT-Sicherheit und Haftung, ecolex 2007, 508.
[672] § 14 Abs 1 letzter Satz DSG.
[673] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 14 Anm 4.

Um diesen Zielsetzungen gerecht werden zu können ist idR eine Kombination von organisatorischen, personellen, technischen und baulichen Sicherungsmaßnahmen erforderlich.[674] Dafür hat sich das betreffende Unternehmen va einer Reihe von Prüfragen zu stellen; mit *Dohr/Pollirer* lassen sich idZ acht Prüfungspunkte feststellen: [675]

1. Besteht eine ausdrückliche Festlegung der Aufgabenverteilung?
2. Besteht eine Bindung der Datenverwendung an das Vorliegen gültiger Aufträge?
3. Wurden die Mitarbeiter nachweislich über ihre Pflichten nach dem DSG belehrt?
4. Darf das Rechenzentrum grds nur vom entsprechenden Bedienungs- und Wartungspersonal betreten werden (sog Closed-Shop-Betrieb)?
5. Stehen die Geräte während der Dienstzeit unter Beaufsichtigung?
6. Besteht eine Beschränkung des Zugriffs auf Daten?
7. Wird die Einhaltung der Datensicherheitsmaßnahmen regelmäßig überprüft?
8. Sind die Datensicherheitsvorschriften entsprechend dokumentiert (etwa in einem Datensicherheitshandbuch)?

Va eine Dokumentation iSd Punkt acht wird sich für Unternehmen, deren wesentlicher Geschäftsinhalt die Datenverarbeitung ist, empfehlen. Solcherart ist im Falle von Datenschutzproblemen ein rascher Zugriff auf die erforderlichen Unterlagen und Informationen gewährleistet, um diese zu beheben, Auskünfte an Betroffene oder die DSK zu geben und nicht zuletzt auch beweisen zu können, dass die Datensicherheitsmaßnahmen tatsächlich eingehalten wurden.[676]

Für das Treffen der Datensicherheitsmaßnahmen ist der Auftraggeber oder der Dienstleister verantwortlich (die uU durchaus aufwendige Prüfung der datenschutzrechtlichen Auftraggebereigenschaft kann somit entfallen).[677] Umfasst sind dabei sämtliche Organisationseinheiten des Auftraggebers oder Dienstleisters. Der in § 14 Abs 1 DSG gebrauchte Begriff der Organisationseinheit ist gesetzlich nicht näher

---

[674] *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 81; vgl dazu auch *Dohr/Pollirer/Weiss*, DSG^2 (2002) § 14 Anm 9.
[675] *Dohr/Pollirer*, Datenschutzkonforme Organisation, ecolex 2006, 706.
[676] *Knyrim*, Datenschutzrecht (2003) 230.
[677] *Dohr/Pollirer/Weiss*, DSG^2 (2002) § 14 Anm 2.

definiert, im unternehmerischen Bereich wird sich eine Auslegung nach betriebswirtschaftlichem Verständnis als sachgerecht erweisen.[678]

Auf die im einzelnen zu treffenden (va) technischen Maßnahmen kann aus Gründen der Zielsetzung dieser Arbeit nicht näher eingegangen werden. Exemplarisch kann hier bspw auf die Ausführungen entsprechender Anleitungen zur Umsetzung von Datensicherheitsmaßnahmen wie das österr Informationssicherheitshandbuch[679] oder den (deutschen) Leitfaden IT-Sicherheit[680] hingewiesen werden.

2. Verhältnismäßigkeitsabwägung und Risikoanalyse

Die Datensicherheitsmaßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.[681] Das Unternehmen hat seine Sicherheitsmaßnahmen somit dynamisch an geänderte Umstände anzupassen.[682] Je höher das Risiko einer Datenverwendung ist, desto höher müssen die Sicherheitsvorkehrungen sein.[683]

Insofern wird den sensiblen Daten nach § 4 Z 2 DSG die höchste Schutzwürdigkeit zuzuerkennen sein; eine Stufe darunter sind strafrechtsrelevante Daten iSd § 8 Abs 4 DSG anzusiedeln. Schließlich ergibt sich aus § 18 Abs 2 DSG für bestimmte Datenarten eine gegenüber den nichtsensiblen Daten erhöhte Schutzwürdigkeit, da dieser Bestimmung zufolge bestimmte Datenanwendungen erst nach Vorabkontrolle durch die DSK aufgenommen werden dürfen. Zu denken ist idZ an Datenanwendungen, die eine Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder in Form eines Informationsverbundsystems durchgeführt werden.[684]

---

[678] MwN *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 83.
[679] *BKA* (Hrsg), Informationssicherheitshandbuch 2.3 (Stand 19.3.2009); s http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf.
[680] *Bundesamt für Sicherheit in der Informationstechnik* (Hrsg), Leitfaden IT-Sicherheit (2007); s http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf (19.3.2009).
[681] § 14 Abs 2 letzter Satz DSG.
[682] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 14 Anm 14.
[683] Vgl *Knyrim*, Datenschutzrecht (2003) 229.
[684] *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 90.

Zusammenfassend ist festzuhalten, dass jedenfalls ein bewegliches System besteht, bei dem zur Beurteilung der konkret zu ergreifenden Datensicherheitsmaßnahmen stets auf die Umstände des jeweiligen Einzelfalles Bedacht zu nehmen ist.

3. Konsequenzen der Verletzung von Datensicherheitsmaßnahmen

Im Gegensatz zum Grundrecht nach § 1 DSG räumen die nach § 14 DSG vorgeschriebenen Datensicherheitsmaßnahmen dem Betroffenen keine subjektiven Rechtsansprüche ein. Insofern besteht auch kein Auskunftsrecht des Betroffenen über seine im Rahmen der Sicherheitsmaßnahmen ermittelten personenbezogenen Daten (etwa iZm der Protokollierungspflicht nach § 14 Abs 2 Z 7).

Ungeachtet dessen kann die Nichtbefolgung vorgeschriebener Datensicherheitsmaßnahmen für Unternehmen schwerwiegende Folgen haben.

In einem unternehmensinternen Kontext ist festzuhalten, dass Datensicherheitsmaßnahmen, die vom Auftraggeber oder Dienstleister erlassen wurden, Dienstanweisungen darstellen. Deren Verletzung durch Mitarbeiter kann dabei arbeitsrechtliche Folgen bis zur Kündigung und Entlassung nach sich ziehen. Wurden die Sicherheitsmaßnahmen von der Unternehmensleitung entsprechend veranlasst, können Mitarbeiter bei einer vorsätzlichen oder grob fahrlässigen Missachtung dieser Bestimmungen auch selbst schadenersatzpflichtig werden.[685]

Für die jeweiligen Unternehmen selbst beachtlich ist der Umstand, dass sich diese neben einer drohenden Verwaltungsstrafe nach § 52 Abs 2 Z 4 DSG [686] va auch dem Risiko einer wettbewerbsrechtlichen Klage ausgesetzt sehen können.
Dies unter der Voraussetzung, dass der Gesetzesverstoß subjektiv vorwerfbar ist und geeignet ist, dem Verletzer einen sachlich nicht gerechtfertigten Vorsprung vor gesetzestreuen Mitbewerbern zu verschaffen.[687]

---

[685] IdS *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 100.
[686] S Kap VI.B.3.
[687] MwN *Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004, 55; s Kap IV.B.7.

B. Das Datengeheimnis

1. Verpflichteter Personenkreis

Gem § 15 Abs 1 DSG haben Auftraggeber, Dienstleister und ihre Mitarbeiter Daten aus Datenanwendungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten geheim zu halten, soweit kein rechtlicher Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht.

Eine Durchbrechung der Geheimhaltungspflicht ist daher nur dann zulässig, wenn auch eine Übermittlung rechtmäßig vorgenommen werden darf; andernfalls sind die Daten immer geheim zu halten.[688]

Von der Verschwiegenheitspflicht betroffen sind all jene Personen, denen berufsmäßig Daten anvertraut wurden oder zugänglich gemacht worden sind. Somit sind nicht nur Personen aus dem eigenen Betrieb eines Unternehmens erfasst, sondern auch solche, die (zeitweise) extern zugezogen wurden. In der wirtschaftlichen Praxis ist bei diesbezüglichen Verträgen (wie bspw mit einem Dienstleister zur Einrichtung eines elektronischen Datenraums) daher die Aufnahme einer Bestimmung von Bedeutung, wonach die Dienstleistungsfirma nur solche Mitarbeiter entsenden darf, die ihr gegenüber auf das Datengeheimnis verpflichtet worden sind anzuraten.[689]

Für die beigezogenen Personen bleiben sonstige berufsspezifische Verschwiegenheitspflichten freilich aufrecht (iZm mit Due Diligence Prüfungen sind hier bspw § 9 Abs 2 RAO und § 91 WTBG zu erwähnen).[690]

---

[688] *Knyrim*, Datenschutzrecht (2003) 231.
[689] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 8.
[690] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 7.

2. Die spezifische Bedeutung des Datengeheimnisses für Übermittlungen

Vor dem Hintergrund der in dieser Arbeit bereits behandelten Problemkreise interessieren nun va die Fragestellungen, die sich iZm Übermittlungen aus den Vorschriften zum Datengeheimnis ergeben können.

Aus § 15 Abs 2 erster Satz DSG ergibt sich, dass Daten nur aufgrund einer ausdrücklichen Anordnung des Arbeitgebers, Auftraggebers und Dienstleisters übermittelt werden dürfen.[691] Dies bedeutet jedoch nicht, dass für jede einzelne Übermittlung eine neue Anordnung erforderlich ist. Die Festlegung der Fälle, in denen eine Übermittlung zulässig ist kann (und wird aus Praktikabilitätsgründen wohl auch anzuraten sein) vielmehr bereits im Vorhinein erfolgen.[692] Bevor ein solcher Übermittlungsauftrag erteilt wird, hat der jeweilige Auftraggeber jedoch stets zu überprüfen, ob die generellen Voraussetzungen[693] für eine Übermittlung gegeben sind.[694]

Auftraggeber und Dienstleister haben ihre Mitarbeiter, sofern eine solche Anordnung nicht bereits kraft Gesetzes[695] besteht, vertraglich zur Einhaltung des Datengeheimnisses zu verpflichten sowie sie über die Folgen einer Verletzung des Datengeheimnisses zu belehren.[696]

Für Unternehmen sind aus den Vorschriften zum Datengeheimnis zusammenfassend va zwei Verhaltensanforderungen relevant: Erstens dürfen Mitarbeiter nur auf Grund ausdrücklicher Anordnung des Aufraggebers Daten übermitteln, wobei diese Anordnungen rechtmäßig sein müssen und sich Mitarbeiter bei rechtswidrigen Anordnungen ohne Nachteile[697] weigern können Daten zu übermitteln; zweitens haben Arbeitgeber ihre Mitarbeiter vertraglich zur Einhaltung des Datengeheimnisses zu verpflichten und über den Datenschutz im Allgemeinen und den Ablauf der Datenverarbeitungen im eigenen Unternehmen zu belehren.[698]

---

[691] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 9.
[692] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 171.
[693] § 7 Abs 2 DSG.
[694] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 13.
[695] Vgl idZ etwa das Kommunikationsgeheimnis nach § 93 Abs 2 TKG.
[696] § 15 Abs 2 zweiter Satz DSG.
[697] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 14.
[698] *Knyrim*, Datenschutzrecht (2003) 232.

Zwar herrscht auch im Arbeitsvertragsrecht grds Formfreiheit, für eine Verpflichtungserklärung wird sich jedoch zur besseren Klarheit (und va auch für Beweiszwecke) die Schriftform empfehlen.[699] In der unternehmerischen Praxis wird dabei neben der Möglichkeit der Unterfertigung einer eigenen Verpflichtungserklärung auch eine Integrierung in den jeweiligen Arbeits- bzw Dienstvertrag praktikabel sein.[700]

3. Konsequenzen einer Verletzung des Datengeheimnisses

Eine Verletzung des Datengeheimnisses ist gem § 52 Abs 1 Z 2 DSG mit Geldstrafe bedroht. Für eine datenschutzkonforme Unternehmensorganisation ist idZ auch beachtlich, dass etwa die Unterlassung der Einholung von Verpflichtungserklärungen der Mitarbeiter bereits ein gröbliches Außerachtlassen der Datensicherheitsmaßnahmen nach § 14 DSG darstellen kann und somit strafbar ist.[701]

Adressaten dieser Strafdrohung sind dabei alle zur Wahrung des Datengeheimnisses Verpflichteten; iE daher alle Mitarbeiter von Auftraggebern oder Dienstleistern, die dem Datengeheimnis unterliegen. Für Unternehmen als juristische Personen bedeutet dies, dass die Strafdrohung insb über den durch § 9 VStG definierten Personenkreis hinausgeht.

Neben verwaltungstrafrechtlichen Folgen können Verletzungen des Datengeheimnisses auch schadenersatzrechtliche Ansprüche der Betroffenen nach sich ziehen. Darüber hinaus sind auch arbeitsrechtliche Konsequenzen (bis hin zur Entlassung) denkbar.[702]

---

[699] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 11.
[700] Vgl *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 104.
[701] Vgl *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 69.
[702] *Jahnel*, Datensicherheit und Datengeheimnis in *Jahnel/Siegwart/Fercher* (Hrsg) Aktuelle Fragen des Datenschutzrechts (2007) 105; *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 15 Anm 15.

VIII. Datenschutz im Arbeitsverhältnis

Abgesehen von den speziellen Implikationen iZm mit Whistleblowing-Hotlines[703] stellen sich beim Schutz von (personenbezogenen) Daten auch im arbeitsvertraglichen Kontext zahlreiche Fragen. Vorrangig sind dies freilich solche, die aus der Kontrollbefugnis des Arbeitgebers bzw der Kontrollunterworfenheit des Arbeitnehmers resultieren.

Dabei zeigt sich va, dass sich regelmäßig die Kontroll- bzw Informationsinteressen des Arbeitgebers auf der einen sowie die schützenswerte Persönlichkeitssphäre des Arbeitnehmers auf der anderen Seite gegenüberstehen.[704] In der Lit sind bislang va jene Bereiche untersucht worden, in denen es um eine Kontrolle des Arbeitnehmers geht (dies ua mit einem Schwerpunkt auf den jeweiligen technischen Verfahren).[705]

Im Folgenden wird der Schwerpunkt der Untersuchung jedoch weniger auf eine kasuistische Darstellung einzelner datenschutzrechtlich relevanter Sachverhalte gelegt, als auf das Aufzeigen grds Lösungsmöglichkeiten.

A. Die gesetzliche Determinierung des Schutzes personenbezogener Daten im Arbeitsverhältnis

1. § 16 ABGB als Grundlage der Arbeitnehmer-Persönlichkeitsrechte

Als ganz grundlegende Norm zur Lösung des Spannungsfeldes zwischen Informationsbedürfnis des Arbeitgebers einerseits und dem Informationsschutz des Arbeitnehmers andererseits stellt sich die Bestimmung des § 16 ABGB dar. Diese bildet neben der arbeitsrechtlichen Fürsorgepflicht und dem Grundrecht auf Datenschutz (dazu gleich mehr) die Rechtsgrundlage bei Fragestellungen im Arbeitsverhältnis iZm mit der

---

[703] S dazu Kap VI.A.3.

[704] *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 288.

[705] Vgl dazu ua *Sacherer*, Datenschutzrechtliche Aspekte der Internetnutzung von Arbeitnehmern, RdW 2005, 221; *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004, 29; *Löschnigg*, Biometrische Daten und Arbeitverhältnis – Zur Zulässigkeit betrieblicher Zutrittskontrollsysteme mittels biometrischer Daten, ASok 2005, 37; *Maurer* biometrische Arbeitszeiterfassung durch Fingerscanner, RdW 2007, 371; *Laimer/Mayr*, Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV- Nutzung, DRdA 2003, 410; vgl idZ auch *Dohr/Pollirer/Weiss*, DSG^2 (2002) Anh V/17, 419 (421).

Menschenwürde.[706] Diese Generalklausel bereitet gleichsam den Weg für grundrechtliche Wertungen der Verfassungsrechtordnung; insofern sind auch grundrechtliche Vorschriften wie jene des Art 8 EMRK im arbeitsvertraglichen Verhältnis anwendbar.[707]

Generell hat bei sämtlichen Maßnahmen[708], die personenbezogene Daten eines Mitarbeiters und somit etwaige schutzwürdige Geheimhaltungsinteressen betreffen können, eine Güter- und Interessenabwägung stattzufinden; dies entspricht auch der traditionellen Grundrechtsdogmatik.[709] Dabei werden den schutzwürdigen Persönlichkeitsrechten des Arbeitnehmers die Informations- oder Kontrollinteressen des Arbeitgebers gegenübergestellt. Die Feststellung der Interessen hat nur nach objektiven Kriterien zu erfolgen, insb was für die Definition der Interessen des Arbeitgebers gilt.[710]

Maßgeblich ist daher, inwieweit der Arbeitgeber nach einem objektiven Maßstab unter Berücksichtigung des konkret in Aussicht genommenen bzw vereinbarten Arbeitsvertrages zur sinnvollen Ausübung seiner vertraglichen Rechte die im Hinblick darauf bekanntzugebenden Informationen tatsächlich benötigt.[711] Kommt man zu dem Ergebnis, dass das Informationsinteresse des Arbeitgebers überwiegt, kann dieser dennoch nicht in beliebiger Weise in Persönlichkeitsrechte des Arbeitnehmers eingreifen. Nach dem Prinzip der Verhältnismäßigkeit muss das gelindeste Mittel mit der geringstmöglichen Eingriffsintensität gewählt werden.

Der Arbeitgeber hat bei der Einrichtung entsprechender Informations- bzw Kontrollsysteme somit zwei Aspekte zu beachten: zum einen muss er ein sachliches und legitimes Kontrollziel verfolgen, zum anderen muss die avisierte Kontrollmethode auch dem Grundsatz der Verhältnismäßigkeit entsprechen.[712]

---

[706] IdS auch *Sacherer*, Internet am Arbeitsplatz als zustimmungspflichtige Kontrollmaßnahme? RdW 2005, 627.
[707] Vgl dazu auch *Brodil*, Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis. Kontrollbefugnisse des Arbeitgebers zwischen Datenschutz und Persönlichkeitsrechten, ZAS 2004, 28.
[708] Durch die Maßnahme muss daher iE eine Datenverwendung iSd § 4 Z 8 DSG verwirklicht werden.
[709] *Aicher* in *Rummel* (Hrsg), ABGB I^3 (2004) § 16 Rz 27.
[710] *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 289.
[711] *Brodil*, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in *Resch* (Hrsg), Die Kontrolle des Arbeitgebers vor dem Hintergrund moderner Medien, 74.
[712] Vgl *Binder*, Detektiveinsatz und Arbeitnehmerkontrolle, in FS Tomandl (1998) 11.

2. Der Schutz von Arbeitnehmer-Persönlichkeitsrechten durch das DSG

Unstrittig ist, dass das DSG ist auf jede Verwendung personenbezogener Daten im Arbeitsverhältnis anzuwenden ist; Datenschutz ist jeher an sich Bestandteil des im Arbeitsverhältnis aus der Fürsorgepflicht des § 16 ABGB erfließenden Schutzes der Privatsphäre des Arbeitnehmers.[713] Insofern wird durch das DSG ein zwar umfangreicher, aber dennoch bloßer Teilbereich der Persönlichkeitsrechte des Arbeitnehmers abgedeckt.[714]

Als va auch im arbeitsrechtlichen Bereich geltender Grundsatz stellt sich das datenschutzrechtliche Prinzip von Treu und Glauben[715] dar. Aus diesem ergibt sich ua die Verpflichtung eines Auftraggebers Daten nur für eindeutige und rechtmäßige Zwecke[716] zu verwenden sowie den Betroffenen zur Erleichterung der Wahrung seiner Rechte darüber auch entsprechend zu informieren.[717]

In Hinblick auf etwaige Einschränkungen folgt auch im Anwendungsbereich des DSG bereits aus der Systematik als Grundrecht die Erfordernis einer Verhältnismäßigkeitsprüfung.[718] Ein Recht auf Geheimhaltung seiner personenbezogenen Daten kann dem Arbeitnehmer daher nur insoweit zukommen, als dieser ein schutzwürdiges Interesse daran hat. *Brodil*[719] zufolge unterscheidet sich das normative System des Datenschutzrechts in der dogmatischen Grundstruktur nicht vom System des § 16 ABGB. In beiden Fällen seien die Informations-, Erhebungs- und Kontrollinteressen nach einem objektiven Maßstab zu erfassen und den schutzwürdigen Geheimhaltungsinteressen des Arbeitnehmers gegenüberzustellen.

Dieser Ansicht ist mE grds zu folgen; zu ergänzen ist jedoch, dass nach dem DSG ausnahmsweise auch solche Geheimhaltungsinteressen für schutzwürdig zu erachten

---

[713] *Brodil*, Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis. Kontrollbefugnisse des Arbeitgebers zwischen Datenschutz und Persönlichkeitsrechten, ZAS 2004, 28.
[714] IglS *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 291.
[715] § 6 Abs 1 Z 1 DSG; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 130.
[716] MwN *Hüttenberger*, Die Bedeutung des Datenschutzes für das Arbeitsrecht, in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 32.
[717] *Stärker*, Datenschutzgesetz, Gesetzestext mit Anmerkungen (2008) § 24 Anm 1.
[718] Vgl *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 48 Rz 61.
[719] *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 292.

sein können, die in der spezifischen (maW subjektiven) Interessenlage des Betroffenen begründet liegen.[720]

B. Modelle für die Datenschutzkonformität betrieblicher Maßnahmen im Arbeitsverhältnis

Vor dem Hintergrund des § 16 ABGB werden betriebliche Kontrollmaßnahmen (wie auch sonst jegliche Informationsbeschaffung) stets als Eingriff in die Privatsphäre des Arbeitnehmers zu beurteilen sein. Voraussetzungen für dessen konkrete Zulässigkeit werden einerseits eine diesbezügliche Information gem § 24 DSG an den betroffenen Arbeitnehmer, andererseits das Vorliegen eines überwiegenden Interesses des Arbeitgebers am jeweiligen Eingriff iSd § 8 Abs 1 Z 4 DSG sein. Insofern ist ein Zugriff in all jenen Fällen ausgeschlossen, in denen kein sachlicher Zusammenhang mit der vertraglich geschuldeten Leistung bzw kein legitimes Kontrollinteresse vorliegt.[721]

So besteht bspw kein generelles Zugriffsrecht auf private Dateien, auch wenn diese etwa auf Hardwarekomponenten des Dienstgebers gespeichert sind. Wie oa ist ein objektiviertes Kontrollziel erforderlich; entstehen im Zuge derart legitimierter Kontrollen beim Arbeitgeber der Verdacht auf einen privaten Charakter abgespeicherter Informationen, ist soweit möglich der Arbeitnehmer zunächst persönlich zu befragen.

1. Verhältnismäßigkeit als Maxime von Kontrollmaßnahmen

Umfang und Ausmaß von Maßnahmen zur Kontrolle von Mitarbeitern werden stets im Rahmen einer Verhältnismäßigkeitsprüfung zu beurteilen sein.

Will ein Unternehmen bspw die Einhaltung eines allgemeinen Privatnutzungsverbotes des Internetzuganges überwachen, kann dies ohne weiteres auch mit gelinderen Mitteln erreicht werden, als durch eine uneingeschränkten Erfassung und Auswertung von Logfiles.[722]

---

[720] Vgl dazu ErläutRV 1613 BlgNR 20. GP 48; *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 28 Anm 4.

[721] *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 293.

[722] Darunter sind Daten zu verstehen, die zum Zweck der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden; vgl dazu Art 2 lit b RL 2002/58/EG.

Als Alternative ist etwa an Stichprobenkontrollen oder bei einem konkreten Missbrauchsverdacht an eine Kontrolle des PC-Arbeitsplatzes des jeweiligen Arbeitnehmers zu denken.

Will der Arbeitgeber hingegen auch die Arbeitsweise seiner Arbeitnehmer im Internet als solche überwachen, wird er dafür – sofern dies nicht ohnehin wegen einer Verletzung der Menschenwürde rechtswidrig ist – die Zustimmung des Betriebsrates[723] bzw, wenn kein Betriebsrat eingerichtet ist, der Arbeitnehmer selbst benötigen.[724]

2. Mögliche Legitimierungen von Kontrollmaßnahmen

Gerade die Überprüfung anhand von Logfiles kann auch geeignet sein, über einzelne Arbeitnehmer sensible Daten zu ermitteln.[725] Deshalb werden solche Datenverwendung stets nur unter den strengen Voraussetzungen des § 9 DSG zulässig sein; dies, da eine Unterscheidung sensibler und nicht sensibler Daten im Vorhinein nicht möglich ist. Insofern kann man von „potentiell sensiblen Daten“ sprechen.[726]

Eine wesentliche Erleichterung für Unternehmen idZ bringt § 9 Z 11 DSG, wonach eine Datenverwendung zur Erfüllung der Rechte und Pflichten eines Auftraggebers auf dem Gebiet des Arbeitsrechts zulässig ist, soweit diese nach den besonderen Rechtsvorschriften zulässig ist.[727]

Im Gros der Fälle wird mE, wenn auch iVm mit einer erforderlichen Zustimmung des Betriebsrates, von der Zulässigkeit der Datenverwendung auszugehen sein, da eine Kontrolle der Arbeitnehmer im Rahmen der Verhältnismäßigkeit idR ein überwiegendes Interesse des Arbeitgebers darstellen wird. Zudem gibt eine entsprechende Information

---

[723] Eine Überwachung der Internetnutzung iS einer inhaltlichen Kontrolle wird idR eine Kontrollmaßnahme iSd § 96 Abs 1 Z 3 ArbVG bedeuten und bedarf somit der Zustimmung des Betriebsrates; idS auch *Dohr/Pollirer/Weiss*, DSG[2] (2002) Anh V/17, 426.
[724] *Sacherer*, Internet am Arbeitsplatz als zustimmungspflichtige Kontrollmaßnahme? RdW 2005, 627.
[725] So lassen sich etwa aus dem Besuch von Internetseiten mit religiösem oder medizinischen Inhalt entsprechende Rückschlüsse ziehen.
[726] *Hattenberger*, Die Bedeutung des Datenschutzes für das Arbeitsrecht, in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 43.
[727] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 9 Rz 14.

der Arbeitnehmer über Kontrollmaßnahmen diesen die Möglichkeit, ihr arbeits- wie privatbezogenes Verhalten am Arbeitsplatz darauf einzustellen.[728]
Zusammenfassend werden sich daher über die übliche datenschutzrechtliche Interessensabwägung sowie eine (besonders im Bereich von Kontrollmaßnahmen gebotene) Zustimmung des Betriebsrates im Einzelfall sachgerechte Entscheidungen treffen lassen.[729] Nichtsdestotrotz muss festgehalten werden, dass die datenschutzrechtliche Fragestellungen im Arbeitsverhältnis nach wie vor äußerst vielfältig sind.

Gerade die große praktische Relevanz von Kontrollmaßnahmen führt in letzter Zeit zu Diskussionen über die Schaffung eigener Arbeitnehmerdatenschutzbestimmungen.[730] Vor dem europarechtlichen Hintergrund des Datenschutzrechts ist zur Vermeidung unterschiedlicher nationaler Schutzniveaus jedoch einmal mehr der europäische Gesetzgeber gefragt.

[728] *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 298.
[729] Vgl dazu *Dohr/Pollirer/Weiss*, DSG[2] (2002) Anh V/17, 417 ff.
[730] S diesbezüglich etwa die Bemühungen des d Bundeskabinetts zur Schaffung einer Grundsatzregelung zum Datenschutz für Arbeitnehmer; s http://www.bundesregierung.de/nn_774/Content/DE/Pressemitteilungen/ BMI/2009/02/2009-02-18-bundeskabinett-beschliesst-grundsatzregelung-zum-datenschutz-der-arbeitnehmer.html (31.3.2009); dazu ehemals krit *Fleck*, Brauchen wir ein Arbeitnehmerdatenschutzgesetz? BB 2003, 306 (310).

IX. Datenschutz im E-Commerce

E-Commerce, oder auch elektronischer Geschäftsverkehr, ist die in der Rechtssprache gebräuchliche Bezeichnung für den elektronischen Handel zwischen Unternehmen[731] bzw zwischen Unternehmen und Verbrauchern.[732] Über den genauen Begriffsumfang besteht dabei kein einheitliches, gefestigtes Verständnis; so enthält insb auch die E-Commerce Richtlinie[733] als europarechtliche Vorgabe dieses Rechtsgebiets keine abschließende Definition dieses Begriffes.

Jedenfalls unbestritten scheint der Kerninhalt dieses Begriffes zu sein, der die Online-Werbung, die Anbahnung und den Abschluss von elektronischen Verträgen im Fernabsatz, das elektronische Signaturrecht, das Fernabsatz-Wettbewerbsrecht sowie das E-Geld-Recht umfasst (E-Commerce ieS).[734]

Bedingt durch die Zielsetzung dieser Arbeit kann im Folgenden nur ein Überblick über ausgewählte, iZm dem E-Commerce auftretende, datenschutzrechtliche Fragestellungen gegeben werden.

A. Datenschutzrechtliche Herausforderungen des E-Commerce

Die für den E-Commerce typische automatische Abwicklung von Geschäftsfällen führt bei den jeweiligen Unternehmen zu immer größeren Mengen von (personenbezogenen) Daten. Bsp reichen von den Warenkorbinformationen der elektronischen Einkaufszettel bis hin zu Systemen zur Finanzbuchhaltung und Lagerverwaltung.[735] Die personenbezogenen Daten stellen idZ eindeutig einen wirtschaftlichen Rohstoff dar, dem ein nicht unerheblicher Wert zukommt (womit insofern auch der Verletzlichkeit des Einzelnen Vorschub geleistet wird).[736]

---

[731] Auch als B2B (Business to Business) bezeichnet.
[732] Auch als B2C (Business to Customer) bezeichnet.
[733] Richtlinie 2000/31/EG des europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl L 178, 1.
[734] *Fina*, Elektronischer Geschäftsverkehr, in *Straube* (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) 78.
[735] *Kramer/Herrmann*, Datenschutz und E-Commerce (2005) 17 Rz 10.
[736] *Wächter*, Datenschutz im Unternehmen (2003) 66 Rz 117.

Im Zuge des elektronischen Geschäftsverkehrs kommt es zu mannigfachen datenschutzrechtlichen Fragestellungen. So kann insb im Hinblick auf die Rechtfertigungstatbestände einer Verwendung personenbezogener Daten, exemplarisch seien etwa die Datenverwendung zu Vetragszwecken[737] sowie die Zustimmung[738] des Betroffenen erwähnt, keine erschöpfende Bearbeitung im Rahmen dieser Arbeit erfolgen.

Im Folgenden wird daher ein Überblick über die jeweiligen Rechte und Pflichten des Leistungen iSd ECG[739] anbietenden Unternehmens einerseits sowie des Nutzers bzw Betroffenen andererseits geboten. Ein Schwerpunkt wird hierbei auf die aus datenschutzrechtlicher Sicht besonders interessierenden Unternehmenspflichten betreffend die Information von Nutzern, Werbemaßnahmen, den Einsatz sog Cookies (dazu gleich mehr) sowie die Informationsrechte des Nutzers bzw Betroffenem im elektronischen Geschäftsverkehr selbst, gelegt.

1. Informationspflichten des Unternehmens im E-Commerce

Gem § 5 ECG sind Angaben über Name oder Firma, geographische Anschrift, Telefon- oder Telefaxnummer, Firmenbuchnummer/Firmenbuchgericht, gegebenenfalls Umsatzsteuer-Identifikationsnummer, zuständige Aufsichtsbehörde, Kammer oder Berufsverband inklusive der anwendbaren gewerbe- oder berufsrechtlichen Vorschriften dem Nutzer leicht und unmittelbar zur Verfügung zu stellen.[740]

Gerade im elektronischen Geschäftsverkehr zeigt sich einmal mehr der hohe Stellenwert zielgerichteter Werbemaßnahmen. Auch idZ haben Unternehmen die Bestimmungen des ECG zu beachten. Als eine der wichtigsten Bestimmungen im oa Zusammenhang ist auf § 6 ECG hinzuweisen.

---

[737] § 8 Abs 3 Z 4 DSG als ein im Bereich des E-Commerce geradezu idealtypischer Rechtfertigungsgrund.
[738] § 8 Abs 1 Z 2 DSG.
[739] Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt und das Signaturgesetz sowie die Zivilprozessordnung geändert werden, BGBl I 2001/ 152.
[740] *Zankl*, Bürgerliches Recht[4] (2008) 175 Rz 262.

Dieser enthält Regelungen betreffend Informationen über kommerzielle Kommunikation und schreibt vor, dass der Anbieter eines E-Commerce-Dienstes dafür zu sorgen hat, dass eine kommerzielle Kommunikation klar und eindeutig

1. als solche erkennbar ist,
2. die natürliche oder juristisch Person, die die kommerzielle Kommunikation in Auftrag gegeben hat, erkennen lässt,
3. Angebote zur Absatzförderung wie etwa Zugaben und Geschenke als solche erkennen lässt und einen einfachen Zugang zu den Bedingungen für ihre Inanspruchnahme enthält sowie
4. Preisausschreiben und Gewinnspiele als solche erkennen lässt und einen einfachen Zugang zu den Teilnahmebedingungen enthält.

2. Die Zulässigkeit von Werbemaßnahmen

Gem § 107 TKG[741] sind Werbemails sowie das Versenden von SMS grds ohne vorherige Einwilligung des Empfängers unzulässig, sofern diese zu Zwecken der Direktwerbung erfolgen oder an mehr als 50 Empfänger gerichtet sind. Grds darf Direktwerbung per E-Mail oder SMS an Verbraucher nur bei einer vorherigen Einwilligung des Verbrauchers erfolgen. In bestimmten Fällen ist eine vorangegangenen Zustimmung jedoch nicht erforderlich: So zB wenn der Absender die Kontaktdaten für die Nachricht iZm dem Verkauf oder einer Dienstleistung an seine Kunden erhält.[742]

Dies bedeutet iE, dass immer dann wenn ein Kunde ein Produkt gekauft hat (oder zumindest ein entsprechendes Interesse daran gezeigt hat) und seine E-Mail-Adresse angegeben hat, dessen Kontaktadresse vom Unternehmen zur Direktwerbung für ähnliche Produkte oder Dienstleistungen verwendet werden darf. Voraussetzung hierfür ist allerdings, dass der Kunde bei der ersten Erhebung und bei jeder weiteren Werbe-E-Mail die Möglichkeit hat, kostenlos und einfach jede weitere Werbung per E-Mail abzulehnen.

[741] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 2003/70 idF BGBl I 2005/133.
[742] Vgl § 7 Abs 3 ECG.

Ein Unternehmen darf die E-Mail-Adresse eines Kunden daher nicht nur zur Vertragserfüllung, sondern auch für Werbung ohne Zustimmung des Kunden verwenden. Zu beachten ist, dass dies nur das jeweilige Unternehmen darf, bei dem der Kunde ein Produkt gekauft hat und dies nur für ähnliche Produkte oder Dienstleistungen zulässig ist.[743]

§ 7 ECG enthält weiters Regelungen über nicht angeforderte kommerzielle Kommunikation. Nach § 7 Abs 1 ECG hat ein Diensteanbieter, der eine kommerzielle Kommunikation zulässigerweise ohne vorherige Zustimmung des Empfängers mittels elektronischer Post versendet, dafür zu sorgen, dass die kommerzielle Kommunikation bei ihrem Eingang beim Nutzer klar und eindeutig als solche erkennbar ist. Jedenfalls unzulässig ist das Versenden elektronischer Post zu Zwecken der Direktwerbung, wenn die Identität des Absenders verschleiert oder verheimlicht wird, oder keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.[744]

§ 7 Abs 2 ECG sieht vor, dass die Rundfunk und Telekom Regulierungs-GmbH eine Liste zu führen hat, in die sich diejenigen Personen und Unternehmen kostenlos eintragen können, die für sich die Zusendung kommerzieller Kommunikation im Weg der elektronischen Post ausgeschlossen haben, und die in Abs 1 genannten Diensteanbieter haben diese Liste zu beachten.[745] Für Unternehmen als Diensteanbieter wird daher darauf zu achten sein, dass diese Liste zur Einsicht verfügbar ist, um etwa eine Zusendung von Werbemails an auf der Liste angeführte Personen zu vermeiden.

Das ECG sieht abgesehen davon auch noch Sondervorschriften für die kommerzielle Kommunikation für Angehörige geregelter Berufe[746] vor und enthält Sonderregelungen über Informationen, die Kunden bei Vertragsabschlüssen im Wege des E-Commerce zu geben sind, über die Abgabe der Vertragserklärung[747] und über die Zugänglichkeit von AGB im E-Commerce.[748]

---

[743] *Knyrim*, Datenschutzrecht (2003) 208.
[744] Sog „opt-out"; s dazu *Zankl*, Bürgerliches Recht[4] (2008) 176 Rz 262
[745] Sog Robinson-Liste; *Zankl*, E-Commerce-Gesetz (2002) 111 Rz 121; s dazu auch § 151 Abs 9 GewO bzw Kap IV.B.8.
[746] § 8 ECG; s dazu die Aufzählung in Art 2 lit g RL 2000/31/EG; zu deren demonstrativem Charakter im österr ECG vgl ErläutRV 817 BlgNR 21. GP 25 (26).
[747] § 10 ECG.
[748] § 11 ECG.

3. Datenschutzrechtliche Anforderungen an den Einsatz von Cookies

In der unternehmerischen Praxis besonders bedeutsame datenschutzrechtliche Fragestellungen werden im Bereich des E-Commerce va iZm Cookies[749] diskutiert. Da andernfalls keine datenschutzrechtliche Relevanz besteht, beziehen sich die folgenden Ausführungen dabei ausschließlich auf Cookies mit zumindest indirektem Personenbezug[750].

Maßgebliche Vorgabe aus dem Europarecht ist Art 5 Abs 3 RL 2002/58/EG: Diesem zufolge ist eine Verwendung von Cookies jedenfalls dann zulässig, wenn dies unbedingt erforderlich ist, um den gewünschten Dienst zur Verfügung zu stellen oder dadurch die Nachrichtenübertragung erleichtert wird.[751] Darüber hinaus ist die Verwendung von Cookies jedoch nur zulässig, wenn der Nutzer oder Kommunikationsteilnehmer über den Zweck der Verarbeitung informiert wird und auf sein Recht diese Verarbeitung zu verweigern, hingewiesen wird.[752]

Die in Bezug auf Cookies vom österr Gesetzgeber getroffenen Bestimmungen stellen sich bei näherer Betrachtung bedauerlicherweise jedoch als wenig klar dar. Im Unterschied zur RL 2002/58/EG ist gem § 96 TKG die Informationspflicht betreffend den Einsatz von Cookies auf den Anbieter[753] beschränkt – dies ist nur der Betreiber eines öffentlichen Kommunikationsdienstes – was gerade die Content-Provider[754] als typische Benutzer von Cookies ausschließt. So löst bspw ein Cookie, das während eines Einkaufvorganges in einem Internet-Shop den Warenkorb speichert, keine Informationspflicht nach dem TKG aus.

Dies widerspricht iE den Vorgaben der RL 2002/58/EG und nicht zuletzt auch dem datenschutzrechtlichen Grundprinzip auf informationelle Selbstbestimmung. Der Einsatz von Cookies soll gerade nur dann zulässig sein, wenn der Nutzer klare und

---

[749] Zu diesem Begriff s Kap IV.C.1.
[750] Im Hinblick auf einen Personenbezug ist im E-Commerce va an den mittlerweile weit verbreiteten Internet-Einkauf mittels „Warenkorb“ zu denken.
[751] Vgl dazu *Knyrim*, Datenschutzrecht (2003) 210; mwN *Jahnel*, Spamming, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108.
[752] S § 96 Abs 2 und 3 TKG.
[753] Zur Legaldefinition s § 92 Abs 3 Z 1 TKG.
[754] Zu den jeweiligen Povider-Typen s http://www.internet4jurists.at/provider/provider1a.htm (14.4.2009).

eindeutige Informationen über deren Zweck erhält.[755] Der Nutzer muss somit wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden und die Gelegenheit haben, die Speicherung von Cookies abzulehnen. Durch die Einschränkung der Informationspflicht auf den Anbieter ist dies jedoch gerade nicht gewährleistet.[756]

Insb aus Sicht der Nutzer bzw Betroffenen im elektronischen Geschäftsverkehr sollte jedoch gewährleistet sein, dass die Informationspflicht beim Einsatz von Cookies auch diejenigen trifft, die diese überwiegend zum Einsatz bringen. Eine entsprechende Klarstellung des gesetzlichen Wortlautes ist mE daher ebenso angebracht wie sinnvoll.

4. Informations- und Auskunftsrechte des Betroffenen bzw Nutzers

Als wesentliches Betroffenenrecht im E-Commerce stellt sich das Auskunftsrecht dar. Da Belange des Datenschutzes vom ECG unberührt bleiben,[757] bildet § 26 DSG die maßgebliche Rechtsgrundlage für die Erteilung von Auskünften über personenbezogene Daten im elektronischen Geschäftsverkehr. § 26 DSG stellt sich dabei als Ausführungsvorschrift zu dem schon in § 1 Abs 3 DSG gewährten Grundrecht auf Auskunft dar.[758]

Das Unternehmen hat dem Nutzer in seiner Eigenschaft als datenschutzrechtlich Betroffenem Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist.[759] Verletzungen der Auskunftspflicht (einschließlich ungerechtfertigter Kostenforderungen oder Mitwirkungswünsche) können dabei mit Beschwerde an die DSK bekämpft werden.[760] Zuwiderhandlungen gegen einen Bescheid der DSK aufgrund einer solchen Beschwerde werden als Verwaltungsübertretungen gem § 52 Abs 1 Z 3 DSG verfolgt.[761]

---

[755] Vgl ErwG 25 RL 2002/58/EG.
[756] *Jahnel*, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004, 21.
[757] *Zankl*, E-Commerce-Gesetz (2002) 77 Rz 57.
[758] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 26 Anm 2.
[759] § 26 Abs 1 DSG.
[760] § 31 Abs 1 DSG.
[761] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 102.

B. Konsequenzen für die Unternehmenspraxis im E-Commerce

Insb für Unternehmen deren Haupt- oder vorrangiger Geschäftsbereich im E-Commerce liegt wird es im Hinblick auf den rechtskonformen Umgang mit Nutzern bzw Betroffenen wichtig sein, bereits bei der Einrichtung einer Datenanwendung die Vorgehensweise bei der Erledigung eines Auskunftsbegehrens durch einen Nutzer ihrer Dienste festzulegen. So kann es zu einem solchen Begehren bspw in Fällen von potentiell unerwünschten Werbemaßnahmen aber auch im Zuge einer Beanstandung der vom Unternehmen erbrachten elektronischen Dienstleistungen kommen.

IE wird es mE daher ratsam sein, schon in Zustimmungserklärungen oder Privacy Policies eine entsprechende Anlaufstelle anzugeben. Andernfalls besteht das Risiko, dass das Auskunftsbegehren verloren geht oder unerledigt bleibt, da dessen Bedeutung verkannt wird, was neben negativen wirtschaftlichen Auswirkungen durch sich schlecht betreut fühlende Kunden va auch zu einem Einschreiten der DSK[762] führen kann.

Schließlich sollte unternehmensintern sichergestellt werden, dass die erforderlichen Auskünfte überhaupt erteilt werden können und es somit organisatorisch nachvollziehbar sein muss, an wen die Daten des Auskunftssuchenden übermittelt wurden oder durch welchen Dienstleister diese verarbeitet werden.[763]

[762] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz, (2000) 230.
[763] IglS *Knyrim*, Datenschutzrecht (2003) 226.

X. Exkurs: Public Sector Information

Im folgenden Kap wird nun eine kurze Darstellung des Bereichs der sog Public Sector Information geboten. Darunter sind generell Informationen des öffentlichen Sektors zu verstehen und zwar unabhängig davon, ob sie einen Personenbezug aufweisen oder nicht.

A. Privatwirtschaftliche Interessen an staatlichen Informationen

1. Informationen des Staates als Wirtschaftsgut

Zunächst ist es erforderlich, dass sich staatliche Informationen überhaupt als handelbares Gut einordnen lassen. Eine derartige Einordnung gelingt jedoch ohne weiteres. Dies, da (wie im Rahmen dieser Arbeit bereits mehrfach aufgezeigt) Informationen an sich unzweifelhaft schon durch die Abhängigkeit wirtschaftlicher Entscheidungsprozesse von den ihnen zur Verfügung stehenden Informationen einen Wert enthalten.

Dies gilt für Informationen des Staates umso mehr. Aufgrund der Vielfältigkeit staatlicher Aufgabenerfüllung werden Informationen mit ebenso vielfältigen gesellschaftlichen Bezügen gesammelt, verarbeitet und gespeichert. Der öffentliche Sektor erfasst, erstellt, reproduziert und verbreitet Informationen ua in den Bereichen Soziales, Wirtschaft, Geographie, Wetter, Tourismus, Geschäftsleben, Patentwesen und Bildung.[764] Für die unterschiedlichen Interessensrichtungen – eben auch Privater – kann der Informationsbestand des Staates daher eine wirtschaftlich nutzbare Ressource darstellen.[765]

2. Wirtschaftlich motivierte Informationsrechte

Abgesehen von den ao Bestrebungen seitens Unternehmen der Privatwirtschaft an staatliche Informationen zu gelangen, existieren jedoch auch Informationen, die für das

[764] *Weissenböck/Knyrim*, IWG (2007) 20.
[765] *Püschel*, Informationen des Staates als Wirtschaftsgut in *Garstka/Kloepfer/Schoch* (Hrsg), Beiträge zum Informationsrecht XVIII (2006) 48 (50).

wirtschaftliche Zusammenspiel von Marktakteuren derart wichtig sind, dass der Gesetzgeber selbst bereits entsprechende Zugangsrechte geschaffen hat.

Um wirtschaftliche Zwecke zu verfolgen, kann so zB auf Informationen des Firmenbuchs, des Grundbuchs oder öffentlich zugänglicher Schuldnerverzeichnisse zurückgegriffen werden.[766] Die Rechtsordnung hat hier offenkundig ein wirtschaftliches Interesse als Legitimation bestimmter Auskunftsansprüche ausdrücklich anerkannt.[767]

Die solcherart erlangten Informationen dienen in weiterer Folge als Entscheidungsgrundlage für bspw den Erwerb eines Baugrundes in einem Industriegebiet, der Gründung eines Unternehmens selbst oder der Überprüfung der Bonität eines potentiellen Geschäftspartners. IE muss Informationen daher keine unmittelbare Wirtschaftsfunktion innewohnen, um selbst zum Wirtschaftsgut zu werden.[768]

B. Gesetzliche Grundlagen einer wirtschaftlichen Nutzung staatlicher Informationen

1. Europarechtliche Grundlagen zum Schutz staatlicher Informationen

Maßgebliche europarechtliche Vorgabe zum Informationsweiterverwendungsrecht in Österreich ist die RL 2003/98/EG.[769] Ziel der Richtlinie ist es, die nationalen Bestimmungen und Verfahren der Mitgliedstaaten für die Weiterverwendung von Dokumenten öffentlicher Stellen auf ein Mindestniveau anzugleichen, um zu gewährleisten, dass die Bedingungen für die Nutzung solcher Informationen gerecht, angemessen und nicht diskriminierend sind. Nicht zuletzt hat diese Angleichung auch zum Ziel, dass ein reibungsloses Funktionieren des Binnenmarktes und die einwandfreie Entwicklung der Informationsgesellschaft in der Gemeinschaft gefördert werden.[770]

---

[766] So etwa die „Warnliste“ der Banken oder die „Kleinkreditevidenz“.
[767] Vgl dazu ganz grds *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 1 Anm 23.
[768] IglS *Püschel*, Informationen des Staates als Wirtschaftsgut in *Garstka/Kloepfer/Schoch* (Hrsg), Beiträge zum Informationsrecht XVIII (2006) 55.
[769] Richtlinie 2003/98/EG des Europäischen Parlaments und Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors, ABl L 2003/345, 90.
[770] Vgl ErwG 6 RL 2003/98/EG.

Auch die Vermeidung von Wettbewerbsnachteilen, die Unternehmen des europäischen Binnenmarktes gegenüber ihren amerikanischen Konkurrenten haben, die sich ihrerseits auf ein hochentwickeltes und gut funktionierendes System öffentlicher Informationen stützen können, sollen ausgeglichen werden.[771]

Weiters soll die RL 2003/98/EG gewährleisten, dass bei der Verwertung von Informationen des öffentlichen Sektors die gleichen Grundbedingungen für alle Akteure auf dem europäischen Informationsmarkt gelten, dass die Bedingungen für die Verwertung transparenter gestaltet und ungerechtfertigte Marktverzerrungen beseitigt werden und dem Marktteilnehmer Rechtssicherheit geboten wird. Sohin sollen gemeinschaftsweite Dienstleistungen gefördert und zu diesem Zweck Hemmnisse für die Nutzung des wirtschaftlichen Potentials öffentlicher Informationen, die sich aus unterschiedlichen mitgliedstaatlichen Regelungen hinsichtlich deren Nutzung ergeben, beseitigt werden.[772]

2. Das Informationsweiterverwendungsrecht in Österreich – das IWG

In Österreich ist die Weiterverwendung staatlicher Informationen durch das IWG[773] geregelt. Dieses orientiert sich sowohl inhaltlich als auch im Aufbau weitestgehend an der PSI-Richtlinie und zielt va auf die Erleichterung der Weiterverwendung von Dokumenten öffentlicher Stellen ab, um dadurch insb die Erstellung neuer Informationsprodukte und -dienste zu fördern.[774]

In 17 Bestimmungen stellt das Gesetz Mindestregeln für die Weiterverwendung der Dokumente öffentlicher Stellen auf. Dabei wird grds keine Verpflichtung für öffentliche Stellen normiert, die Verwertung bestimmter Dokumente zu gestatten. Weiters besteht auch keine Verpflichtung solche Dokumente weiterzugeben. Wenn jedoch Dokumente weitergegeben werden, dann hat dies unter Anwendung der Regelungen dieses Gesetzes zu erfolgen.

---

[771] *Weissenböck/Knyrim*, IWG (2007) 22.
[772] ErläutRV 1026 BlgNR 22. GP 2.
[773] Bundesgesetz über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz – IWG), BGBl I 2005/135.
[774] *Knyrim/Weissenböck*, Erste Praxiserfahrungen mit dem Informationsweiterverwendungsgesetz, jusIT 2008, 29.

Die erstmalige Entscheidung, ob eine Weiterverwendung genehmigt wird, ist dabei Sache der betreffenden öffentlichen Stelle. Wurde die Weiterverwendung von Dokumenten aber einmal gestattet, dann sind diese in nicht diskriminierender Weise[775], innerhalb eines bestimmten zeitlichen Rahmens[776], uU gegen angemessenes Entgelt[777] und grds nicht exklusiv auf Antrag[778] auch an jeden Dritten weiterzugeben.

Den öffentlichen Stellen ist eine eigene wirtschaftliche Nutzung ihrer Dokumente gestattet. Werden Dokumente von öffentlichen Stellen als Ausgangsmaterial für eigene wirtschaftliche Geschäftstätigkeiten verwendet, die nicht unter ihren öffentlichen Auftrag fallen, gelten für diese Tätigkeiten dieselben Bedingungen wie für andere Nutzer.[779]

Ohne auf weitere spezifische Fragestellungen eingehen zu können sind es va zwei Kernpunkte die die wesentliche Charakteristik des österr IWG ausmachen: Zum einen der Umstand, dass nach § 2 Abs 1 IWG grds keine Verpflichtung der öffentlichen Stelle besteht, Dokumente zur Weiterverwendung zur Verfügung zu stellen.[780] Zum anderen die Nichtdiskriminierungsbestimmung des § 10 Abs 1 IWG, wonach "Entgelte und sonstigen Bedingungen für die Weiterverwendung von Dokumenten, die sich im Besitz von öffentlichen Stellen befinden", ... "für vergleichbare Kategorien der Weiterverwendung nicht diskriminierend zu sein haben." Öffentliche Stellen sind demzufolge im Rahmen der Genehmigung der Weiterverwendung ihrer Dokumente verpflichtet, vergleichbare Kategorien der Weiterverwendung hinsichtlich der Entgelte und Nutzungsbedingungen gleich zu behandeln.[781]

Für Unternehmen insb von Interesse ist der Umstand, dass sich aus dem Verbot der Diskriminierung nicht zuletzt auch ein durchsetzbarer Anspruch auf Bereitstellung von Dokumenten ableiten lässt.[782]

---

[775] § 10 IWG.
[776] § 5 IWG.
[777] § 7 IWG.
[778] § 11 IWG.
[779] Vgl *Knyrim*, Informationsweiterverwendungsrecht – Chancen und Risiken der (kommerziellen) Weiterverwendung von Informationen der öffentlichen Hand, ÖJZ 2008/4, 18.
[780] *Weissenböck/Knyrim*, IWG (2007) § 1 Anm 2.
[781] *Weissenböck/Knyrim*, IWG (2007) § 10 Anm 5.
[782] Vgl *Weissenböck/Knyrim*, IWG (2007) § 10 Anm 2.

Berührungspunkte zum Datenschutz weist das IWG, das die Bestimmungen des DSG unberührt lässt[783], va bei der Abgrenzung der verschiedenen Zwecke bzw Verwendungskategorien iSd § 10 IWG auf. Die Abgrenzung dieser verschiedenen Verwendungszwecke kann in der Praxis durchaus diffizil sein und ist insofern mit Fragestellungen iZm mit dem Zweckbindungsgrundsatz nach § 6 Abs 2 Z 2 DSG vergleichbar. Dementsprechend wird eine Anwendung der dort entwickelten Methodik auch im Anwendungsbereich des IWG zielführend sein können.[784]

[783] § 2 Abs 3 IWG.
[784] IdS auch *Knyrim*, Informationsweiterverwendungsrecht – Chancen und Risiken der (kommerziellen) Weiterverwendung von Informationen der öffentlichen Hand, ÖJZ 2008/4, 19.

XI. Resümee

A. Zusammenfassung

Wie im Laufe der Arbeit gezeigt werden konnte, ist das Thema Datenschutz im unternehmerischen Alltag allgegenwärtig. Für das Unternehmen idZ relevant sind jedoch nicht nur die Bestimmungen des DSG sondern auch zahlreiche andere (großteils) einfachgesetzliche Vorschriften. So finden sich insb in den gesellschaftsrechtlichen Bestimmungen zur Verschwiegenheitspflicht, den strafrechtlichen Tatbeständen zur Wahrung von Betriebsgeheimnissen oder auch im Wettbewerbsrecht zahlreiche Berührungspunkte mit der Materie Datenschutz.

Verstöße gegen das Datenschutzrecht können dabei neben Verwaltungstrafen va zivilrechtliche Schadenersatzansprüche nach sich ziehen, soweit ein materieller Schaden nachweisbar ist. Auch der aus solchen Verstößen resultierende Imageverlust vermag ein Unternehmen nachhaltig zu schädigen.

Bei den in der wirtschaftlichen Praxis bedeutenden Umstrukturierungen konnte zudem erstmalig für die österr Rechtslage gezeigt werden, dass das Thema Datenschutz weder ein unlösbarer Konflikt zweier Rechtsmaterien, noch (wie zT behauptet) ein künstlich erzeugtes Scheinproblem ist.[785] IE kann das DSG gesellschaftsrechtliche Umstrukturierungen nicht hindern. Nichtsdestotrotz ist das Datenschutzrecht eine beachtliche Rechtsmaterie und somit auch in allen Phasen der Umstrukturierung zu berücksichtigen.

Auch die Untersuchungen zu Übermittlungen in Konzernstrukturen, den organisatorischen Anforderungen an den Datenschutz im Unternehmen[786], die datenschutzkonforme Ausgestaltung des Verhältnisses Arbeitnehmer – Arbeitgeber[787]

[785] Für die ganz ähnlich gelagerten Fragestellungen in D s dazu (in der grds Bewertung zu einem vergleichbaren Ergebnis kommend) *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 295 ff.
[786] *Dohr/Pollirer*, Datenschutzkonforme Organisation, ecolex 2006, 706.
[787] Vgl *Brodil*, Geheimnisschutz-Informationsschutz-Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz-Informationsschutz-Datenschutz (2008) 288

sowie ausgesuchte Fragestellungen im E-Commerce[788] konnten die Relevanz eines rechtskonformen Umgangs mit personenbezogenen Daten belegen.

Nicht zuletzt die Tätigkeit des Gesetzgebers im Bereich der sog Public Sector Information belegt mittlerweile hinreichend den zunehmenden Stellenwert von (staatlichen) Informationen[789] als Wirtschaftsgut.[790]

Die weiter zu erwartende wachsende Bedeutung des Schutzes personenbezogener Daten wird von Unternehmen daher in Hinkunft einen noch bewußteren Umgang mit dem Datenschutz als Rechtsmaterie verlangen.

B. Abschließende Bewertung und Ausblick

Eine wesentliche Schwierigkeit besteht in den oa Untersuchungen freilich darin, dass allgemein zivilrechtliche, gesellschaftsrechtliche und datenschutzrechtliche Regelungsregime mit ihren typischerweise stark differenzierenden rechtsdogmatischen Ansätzen in Einklang zu bringen sind.

Dass eine Bedachtnahme auf all diese Rechtsgebiete erforderlich ist, konnte va in der Argumentation hinsichtlich der grds Frage, ob gesellschaftsrechtliche Umstrukturierungen überhaupt als datenschutzrechtlich relevanter Vorgang zu qualifizieren sind, gezeigt werden.[791]

Als Kernpunkt der Argumentation ist hier nochmals auf die Ausgestaltung des Datenschutzes als Grundrecht hinzuweisen. Vor diesem Hintergrund ist insb festzuhalten, dass im Einzelnen va keine Übertragung von Rechten an personenbezogenen Daten iS einer Zession möglich ist. Erforderlich ist daher stets eine Prüfung der konkreten Zulässigkeit eines Eingriffs in das Recht des Betroffenen auf Geheimhaltung seiner Daten (iglS auch *Feltl* und der Autor selbst).[792]

---

[788] S *Kramer/Herrmann*, Datenschutz und E-Commerce (2005) 17 Rz 10.
[789] Darunter eben auch personenbezogene Daten.
[790] Vgl dazu *Püschel*, Informationen des Staates als Wirtschaftsgut in *Garstka/Kloepfer/Schoch* (Hrsg), Beiträge zum Informationsrecht XVIII (2006) 48 (50).
[791] Kap V.D.
[792] *Auer/Feltl*, Zur datenschutzrechtlichen Relevanz von Umstrukturierungsvorgängen, SWK 2009, 815 (818).

Das Grundrecht auf Datenschutz steht dabei unter einem materiellen Gesetzesvorbehalt; als zentrales Element im Datenschutzrecht stellt sich in einer Zusammenschau va die Interessensabwägung dar.[793] Dies, da einschlägige Erlaubnistatbestände im Gesetz oftmals nicht vorhanden sind und sich die Verwendung personenbezogener Daten andernfalls gar nicht rechtfertigen ließe.

Jene Fälle in denen die Legitimierung einer Datenverwendung nicht durch überwiegende berechtigte Interessen anderer möglich ist, verlangen schließlich eine entsprechende Zustimmung der Betroffenen.[794]

Zumeist kann sich der für Unternehmen für eine rechtmäßige Datenverwendung erforderliche Aufwand dabei jedoch verhältnismäßig gering gestalten lassen: Wie dargestellt wurde, werden sich viele datenschutzrechtliche Implikationen iE schon durch die schlichte Eliminierung des Personenbezugs lösen lassen.[795]

Des weiteren ist vor dem Hintergrund globalisierter Wirtschaftsbeziehungen für Unternehmen va auf die Rechtskonformität der Übermittlung und Überlassung personenbezogener Daten ins Ausland besonderes Augenmerk zu legen.

So wird zwar die Zulässigkeit einer Datenübermittlung im Zuge einer grenzüberschreitenden Umstrukturierung im europäischen Binnenmarkt im Gros der Fälle keine besonderen Schwierigkeiten aufweisen; treten jedoch Gesellschaften mit Sitz in Drittländern hinzu kann sich ein rechtskonformes Vorgehen unverhältnismäßig komplizierter darstellen. Dies insb wenn die involvierten Rechtsordnungen durch unterschiedliche Datenschutzniveaus gekennzeichnet sind.[796]

---

[793] *Dohr/Pollirer/Weiss*, DSG² I (2002) § 1 Anm 10; *Duschanek*, in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III (1999) 35 Rz 44.

[794] So va bei der Verwendung von sensiblen Daten; vgl dazu etwa die Fragestellungen iZm der Übermittlung solcher Daten im Rahmen von Human Resource Due Diligence Prüfungen.

[795] S dazu die Ausführungen in Kap V.E.6.b).(2); *Dohr/Pollirer/Weiss*, DSG[2] I (2002) § 4 Anm 2; vgl dazu auch *Braun/Wybitul*, Übermittlung von Arbeitnehmerdaten bei Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 786; *Feltl/Mosing*, Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 240; *Fleischer/Körber* in *Berens/Brauner/Strauch* (Hrsg) Due Diligence bei Unternehmensakquisitionen[4] (2005) 296.

[796] Dazu weiterführend *Schröcker*, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006) 18.

Insofern wird das komplexe System von Verweisen des DSG in seiner derzeitigen Ausgestaltung den Ansprüchen nach Rechtssicherheit und Praktikabilität internationaler Transaktionen mE auch nur zT gerecht werden können.[797]

Weiters ist die Umsetzung diesbezüglicher E der EK zum Vorliegen eines angemessenen Schutzniveaus in Drittländern durch den (materiellen) österr Gesetzgeber bis dato noch nicht vollständig erfolgt.[798] Die Schaffung entsprechender Rechtsgrundlagen könnte mE daher eine ebenso sinnvolle wie angezeigte Abhilfe schaffen.[799]

Dass das Thema Datenschutz auch in Zukunft sowohl in der unternehmerischen Praxis als auch in der juristischen Lit weiter an Bedeutung zunehmen wird, ist unbestritten. Meiner Auffassung nach wird sich für involvierte Unternehmen ein engagierter Zugang zum Datenschutz in jedem Fall als ratsam erweisen: Statt als Behinderung im wirtschaftlichen Alltag scheint es vielmehr zweckmäßig ein Akkordieren mit den einschlägigen datenschutzrechtlichen Vorgaben als Wettbewerbsvorteil zu begreifen.[800]

Eine hohe Qualität in der „Datenschutzpolitik“ eines Unternehmens wird nicht zuletzt zu Zufriedenheit und Vertrauen bei den Kunden und Mitarbeitern führen und sich damit auch wirtschaftlich langfristig positiv auswirken.

Ein aufgeschlossener und positiver Umgang von Unternehmen mit dem Thema Datenschutz wird sich daher sowohl aus Gründen des Vermeidens etwaiger negativer Konsequenzen als auch aus einer rein marktwirtschaftlichen Perspektive bezahlt machen.

---

[797] Vgl Kap V.F.3.c)(2).
[798] Vgl die Verordnung des Bundeskanzlers über den angemessen Datenschutz in Drittstaaten (Datenschutzangemessenheitsverordnung – DASV) BGBl II 1999/521.
[799] S Kap V.F.3.b)(1).
[800] S idZ auch *Knyrim*, Datenschutzrecht (2003) 244 (245).

Literaturverzeichnis

Appl, Datenschutzrechtliche Implikationen gesellschaftsrechtlicher Umstrukturierungen, GeS 2008, 96

Arnold, Die Pflicht des Vorstandes zur Auskunftsverweigerung in der Hauptversammlung, GesRZ 2007, 99

Auer/Feltl, Zur datenschutzrechtlichen Relevanz von Umstrukturierungsvorgängen, SWK 2009, 815

Beisel/Klumpp, Unternehmenskauf[5] (2006)

Berens/Brauner/Strauch, Due Diligence bei Unternehmensakquisitionen[4] (2005)

Berka, Geheimnisschutz-Datenschutz-Informationsschutz im Lichte der Verfassung, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 53

Berndt/Hoppler, Whistleblowing ein integraler Bestandteil effektiver Corporate Governance, BB 2005, 2624

Biermann, Kundendaten von Monster.com geplündert, Zeit Online (28.1.2009)

Bihr, Due Diligence: Geschäftsführungsorgane im Spannungsfeld zwischen Gesellschafts- und Gesellschafterinteressen, BB 1998, 1198

Böttcher, Verpflichtung des Vorstands einer AG zur Durchführung einer Due Diligence NZG 2005, 49

Brandl/Hohensinner, Datenschutzrechtliche Aspekte der Tätigkeit von Adressverlagen und Direktmarketingunternehmen, ecolex 2003, 135

Braun/Wybitul, Übermittlung von Arbeitnehmerdaten bei Due Diligence- Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 782

Breitenmoser/Riemer/Seitz, Praxis des Europarechts – Grundrechtsschutz (2006)

Brodil, Geheimnisschutz-Datenschutz-Informationsschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 287

Brodil, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 74

Bünder, Neue Datenpanne bei der Telekom, Frankfurter Allgemeine Zeitung, 26.11.2008

Dohr/Pollirer, Datenschutzkonforme Organisation, ecolex 2006, 706

Dohr/Pollirer/Weiss (Hrsg), Datenschutzgesetz 2000[2] (2002)

Doralt/Nowotny/Kalss, Kommentar zum Aktiengesetz I (2003)

Drobesch/Grosinger, Das neue österreichische Datenschutzgesetz, Kurzkommentar (2000)

Duschanek/Rosenmayr-Klemenz, Datenschutzgesetz 2000, Kurzkommentar (2000)

Duursma/Duursma-Kepplinger/Roth, Handbuch zum Gesellschaftsrecht (2007)

Essers/Hartung, Datenschutz bei Unternehmenstransaktionen, RDV 2002, 278

Fabrizy, Strafgesetzbuch[9], Kurzkommentar (2006)

Fellner, Persönlichkeitsschutz juristischer Personen (2007)

Feltl/Mosing, Das Grundrecht auf Datenschutz bei Verschmelzung und Spaltung, GesRZ 2007, 233

Fleck, Brauchen wir ein Arbeitnehmerdatenschutzgesetz? BB 2003, 306

Fleischer/Körber, Due Diligence und Gewährleistung beim Unternehmenskauf, BB 2001, 841

Flendrovsky/König/Kotschy, Datenschutz – Teil I: Datenschutzkommission (DSK), in *Sachs/Thanner* (Hrsg), Verfahren vor Sonderbehörden (2006) 1

Foregger/Litzka (Hrsg), Mediengesetz[4] (2000)

Frowein/Peukert, EMRK[2], Kommentar (1996)

Gellis/Feil, GmbHG[6], Kommentar (2006)

Genz, Datenschutz in Europa und in den USA (2004)

Gola/Schomerus, BDSG[9], Kommentar (2007)

Graf, Datenschutzrecht im Überblick (2004)

Graf/Riesenhuber, Whistleblowing-Hotline: Bescheid der DSK zu GZ K178.274/0010-DSK/2008 vom 5.12.2008 – Einige gelöste, viele offene Fragen, jusIT 2009, 143

Gran, Abläufe bei Mergers und Acquisitions, NJW 2008, 1409

Hanusch, GewO[2], Kommentar (2003)

Hasberger, IT-Sicherheit und Haftung, ecolex 2007, 508

Hattenberger, Die Bedeutung des Datenschutzes für das Arbeitsrecht, in *Resch* (Hrsg), die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 13

Heidinger/Albeseder, Due Diligence, Handbuch für die Praxis (2001)

Hinterhofer, Geheimnisschutz-Datenschutz-Informationsschutz im Strafrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 169

Hödl, Die Macht der klugen Dinge. Überlegungen zu ubiquitous computing, RFID-Chips und smart objects, juridikum 2007, 210

Hofmann, Due Diligence – Möglichkeiten und Grenzen des Managements (2006)

Holaschke, Einflussfaktoren auf die Bereitschaft persönliche Daten zur Verfügung zu stellen (2007)

Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] (2008)

Jabornegg/Strasser, Kommentar zum Aktiengesetz[4] (2006)

Jahnel, Kein Schutz von Unernehmensdaten nach dem DSG? RdW 2005, 244

Jahnel, Datensicherheit und Datengeheimnis, in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 79

Jahnel, Spamming, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108

Jahnel, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004, 21

Jahnel/Thiele, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004, 55

Kalss, Geheimnisschutz-Datenschutz-Informationsschutz im Gesellschaftsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 237

Kalss/Bachner, Handkommentar Verschmelzung- Spaltung – Umwandlung (1997)

Karner, Der zivilrechtliche Schutz von Geheimnissen, Daten und Informationen, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 135

Kiethe, Vorstandshaftung aufgrund fehlerhafter Due Diligence beim Unternehmenskauf, NZG 1999, 976

Kinscher (Hrsg), Die Gewerbeordnung 1994 mit grundlegender Judikatur der Höchstgerichte sowie verweisenden und erläuternden Anmerkungen unter Heranziehung der Gesetzesmaterialien[13] (2007)

Kittelberger, External Reporting als Pflicht zum Whistleblowing? ÖBA 2007, 90

Klang (Hrsg), Kommentar zum ABGB[2] (1964)

Knyrim, Einspielung österreichischer Kunden- und Mitarbeiterdaten in internationale Konzerndatenbanken: Vorsicht! Die Presse, 31.5.2003

Knyrim, Informationsweiterverwendungsrecht – Chancen und Risiken der (kommerziellen) Weiterverwendung von Informationen des öffentlichen Hand, ÖJZ 2008, 4

Knyrim, Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach! Ecolex 2009, 85

Knyrim/Kurz/Haidinger, Whistleblowing-Hotlines: Mitarbeiter „verpfeifen" zulässig? ARD 2006, 5681

Knyrim/Weissenböck, Erste Praxiserfahrungen mit dem Informationsweiterverwendungsgesetz, jusIT 2008, 29

Koppensteiner/Rüffler, Kommentar zum GmbHG[3] (2007)

Koppensteiner (Hrsg), Österreichisches und europäisches Wettbewerbsrecht[3] (1997)

Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht III (1999)

Kotrnoch, Steuerfragen zur Umwandlung von Kapitalgesellschaften, in *Vodrazka* (Hrsg), Strukturverbesserung – Praxis und Recht, Festschrift für Franz Helbich zum 65. Geburtstag (1990)

Kotschy, Verwaltungsbehördlicher Rechtsschutz in Datenschutzangelegenheiten, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 121

Kotschy/Reimer, Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004, 29

Kozak/Uitz, Virtuelle Daten(t)räume, ecolex 2007, 440

Koziol, Der Grundsatz wonach Daten nur nach Treu und Glauben verarbeitet werden dürfen erfordert eine Benachrichtigung der Betroffenen vor Eintragung in die Warnliste, ÖBA 2006, 530

Koziol/Welser, Bürgerliches Recht I[13] (2006) II[13] (2007)

Kramer/Herrmann, Datenschutz und E-Commerce (2005)

Krejci, Verschwiegenheitspflicht des AG-Vorstands bei Due Diligence Prüfungen, RdW 1999, 574

Krejci, Unternehmensrecht[4] (2008)

Krilyszyn, Unternehmenszusammenschlüsse und Datenschutz, ÖZW 1980, 65

Krüger/Kalbfleisch, Due Diligence bei Kauf und Verkauf von Unternehmen – Rechtliche und steuerliche Aspekte der Vorprüfung beim Unternehmenskauf, DStR 1999, 175

Kunnert, Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009, 102

Laimer/Mayr, Zur Spannung von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, DRdA 2003, 410

Lehner, Whistleblowing-Hotlines gemäß SOX, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 149

Leissler, „Whistleblowing" – die ersten Schritte in Österreich…, ecolex 2009, 361

Löschnigg, Biometrische Daten und Arbeitsverhältnis – Zur Zulässigkeit betrieblicher Zutrittskontrollsysteme mittels biometrischer Daten, ASoK 2005, 37

Lüttge, Unternehmensumwandlung und Datenschutz, NJW 2000, 2463

Marsch-Barner/Mackenthun, Das Schicksal gespeicherter Daten bei Verschmelzung und Spaltung von Unternehmen, ZHR 2001, 165

Maurer, Biometrische Arbeitszeiterfassung durch Fingerscanner, RdW 2007, 371

Mayer-Schönberger/Brandl, Datenschutzgesetz 2000[2] (2006)

Merkt, Due Diligence und Gewährleistung beim Unternehmenskauf, BB 1995, 1041

Nowotny, „Due Diligence" und Gesellschaftsrecht, WBl 1998, 145

Oberndorfer/Trybus, Die (un)überwindbaren Schranken des Datenschutzrechts für Unternehmen mit Fokus auf Informationsverbundsysteme, in *Schweighofer/Geist/Heindl* (Hrsg), 10 Jahre Iris: Bilanz und Ausblick, IRIS 2007, 296

Öhlinger, Verfassungsrecht[7] (2007)

Oppitz, Bankgeheimnis, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 269

Parschalk/Wahl, Ausgewählte Fragen der Gewährleistung beim Unternehmenskauf, WBl 2003, 353

Patzak, Datenschutzrecht für den E-Commerce: Eine rechtsvergleichende Studie der datenschutzrechtlichen Anforderungen in Deutschland und Österreich, dargestellt am Beispiel des Online-Einkaufs (2006)

Philapitsch, Selbstregulierung im Datenschutz, MR 2005, 270

Picot (Hrsg), Handbuch Mergers & Acquisitions (2005)

Püschel, Informationen des Staates als Wirtschaftsgut, in *Garstka/Kloepfer/Schoch* (Hrsg), Beiträge zum Informationsrecht XVIII (2006)

Räther/Seitz, Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425

Reimer, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 183

Reindl, Computerstrafrecht im Überblick (2004)

Reischl, Striptease am Daten, Kurier, 5.10.2008

Reiter/Wittmann-Tiwald (Hrsg), Goodbye Privacy – Grundrechte in der digitalen Welt (2008)

Riegler, Rechtskonforme Übermittlung von Kundendaten (2004)

Ruhm, Haftung des Aufsichtsrates einer AG bei pflichtwidriger Weitergabe von Geschäftsinformationen, RdW 2005, 813

Rummel, Kommentar zum ABGB[3] (2000)

Sacherer, Datenschutzrechtliche Aspekte der Internetnutzung von Arbeitnehmern, RdW 2005, 221

Sacherer, Internet am Arbeitsplatz als zustimmungspflichtige Kontrollmaßnahme? RdW 2005, 627

Schaffland, Datenschutz und Bankgeheimnis bei Fusion – (k)ein Thema? NJW 2002, 1539

Schröcker, Datenschutz und Universalsukzession bei Verschmelzungen nach dem Umwandlungsgesetz (2006)

Schwimann, Praxiskommentar ABGB[3] (2005)

Semler/Stengel, Kurzkommentar zum d Umwandlungsgesetz[2] (2007)

Settele, Das Schlüsselloch Internet – Suchmaschine serviert Personendaten, Neue Zürcher Zeitung, 5.2.2008

Siemen, Datenschutz als europäisches Grundrecht (2006)

Sima/Uitz, Zum Unternehmenskauf ins Internet – Virtueller Datenraum, Die Presse, 16.9.2008

Simitis, BDSG[6], Kommentar (2006)

Simitis, Umwandlungen: ein blinder Fleck im Datenschutz? ZHR 2001, 453

Sina, Zur Berichtspflicht des Vorstandes gegenüber der Aufsichtsrat bei drohender Verletzung der Verschwiegenheitspflicht durch einzelne Aufsichtsratmitglieder, NJW 1990, 1016

Spiegler/Kocina, Ich lass Dich nie mehr alleine…, Die Presse, 29.1.2009

Spill, Due Diligence – Praxishinweis zur Planung, Durchführung und Berichterstattung, DStR 1999, 1787

Spring, Whistleblowing – Verpfeif-Maßnahmen aus datenschutzrechtlicher Sicht, ecolex 2007, 139

Stärker, DSG (2008)

Straube (Hrsg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2006)

Teichmann/Kiesling, Datenschutz bei Umwandlungen, ZGR 2001, 33

Thyri, Geheimnisschutz-Datenschutz-Informationschutz im Wettbewerbsrecht, in *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz Datenschutz Informationsschutz (2008) 217

Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch (2007)

Trybus/Uitz, Datenschutz als Stolperstein für elektronische Due Diligence Prüfungen, MR 2007, 341

Weichert, Datenschutz bei Suchmaschinen, MR-Int 2007, 188

Weissenböck/Knyrim, Kommentar zum IWG (2007)

Wengert/Widmann/Wengert, Datenschutz und Bankenfusionen, NJW 2000, 1289

Wisskirchen/Körber/Bissels, Whistleblowing und Ethikhotlines, BB 2006, 1567

Zankl, Bürgerliches Recht[4] (2008)

Zankl, E-Commerce-Gesetz (2002)

Zib/Verweijen (Hrsg), Das neue Unternehmensgesetzbuch (2006)

Zumbansen/Lachner, Die Geheimhaltungspflicht des Vorstands bei der Due Diligence: Neubewertung im internationalen Geschäftsverkehr, BB 2006, 613

Elektronische Veröffentlichungen

ARGE DATEN
http://www2.argedaten.at/session/anonym242093opojia972491.E42_INP.html
(20.10.2008)

ARGE DATEN, DSK genehmigt Weitergabe von „whistle blowing"-Daten in die USA http://www2.argedaten.at/session/anonym238665oatzzx650535.E42_INP.html
(21.3.2009).

Bundesamt für Sicherheit in der Informationstechnik (Hrsg), Leitfaden IT-Sicherheit (2007) http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf (19.3.2009).

BKA (Hrsg), Informationssicherheitshandbuch 2.3 http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf (Stand 19.3.2009)

Bemühungen des d Bundeskabinetts zur Schaffung einer Grundsatzregelung zum Datenschutz für Arbeitnehmer http://www.bundesregierung.de/nn_774/Content/DE/Pressemitteilungen/BMI/2009/02/2009-02-18- bundeskabinett-beschliesst-grundsatzregelung-zum-datenschutz-der-arbeitnehmer.html (31.3.2009)

OECD http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html (16.11.2008)

ORF.at, Übereifrige Datensammler in Vorarlberg – AK fordert schärfere Datenschutzgesetze http://vorarlberg.orf.at/stories/358395 (28.4.2009)

ORF.at, Neue Hürden für Datenhändler http://futurezone.orf.at/stories/1500676/ (10.12.2008)

ORF.at, Brisantes Datenleck in Deutschland http://orf.at/081213-32774/index.html (13.12.2008)

http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=rotaru&sessionid=15299385&skin=hudoc-en (29.10.2008).

http://www.internet4jurists.at/intern27.htm (17.11.2008).

http://www.gbd-e.org/about.html (31.3.2009).

http://www.gbd-e.org/publications.html (31.3.2009).

Homepage der US Securities and Exchange Comission http://uscode.house.gov/download/pls/15C2A.txt (11.12.2008).

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (6.3.2009).

http://www.truste.org/ (6.3.2009).

http://www.bbb.org/online/ (6.3.2009).

Sarbanes-Oxley Act 2002 http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley (16.3.2002).

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf (16.3.2009).

http://www.internet4jurists.at/provider/provider1a.htm (14.4.2009).

Anhang

A. Informationen gem der VO über die Formvorschriften zur Einreichung von Hochschulschriften, veröffentlicht am 15.07.2008, 42. Stück, Nr 351

1. Zusammenfassung

Die vorliegende Arbeit untersucht Fragestellungen bzw Implikationen, die sich in unternehmerischen Abläufen der wirtschaftlichen Praxis iZm mit dem verfassungsgesetzlich gewährleisteten Recht auf Geheimhaltung personenbezogener Daten stellen können.

Ein Schwerpunkt wird hierbei auf den Vorgang gesellschaftsrechtlicher Umstrukturierungen gelegt. Der Erwerb von Unternehmen, bzw von Anteilen an solchen, gehört in der Wirtschaft mittlerweile zum täglichen Geschäft. Damit gehen zumeist zwangsläufig Veränderungen in den rechtlichen Strukturen der Unternehmen einher, insb werden bei diesen Vorgängen oftmals große Mengen personenbezogener Daten verwendet.

Die für den Kaufinteressenten besonders wichtige Information über die wirtschaftlichen Umstände des entsprechenden Unternehmens erfolgt dabei im Rahmen sog Due Diligence Prüfungen. Im Zuge derer kann gerade die umfassende Zurverfügungstellung personenbezogener Daten wesentliche Voraussetzung für den Erfolg einer geplanten Akqusition sein. Die Untersuchung des datenschutzrechtlichen Schicksals der dabei verwendeten Informationen ist vorrangige Zielsetzung dieser Arbeit; insb wird auseinandergesetzt, ob durch das zivilrechte Institut der Gesamtrechtsnachfolge ein datenschutzrechtlicher Tatbestand erfüllt wird, oder nicht.

Weiters werden besondere Fragestellungen im Konzern erörtert sowie ein Überblick über datenschutzrechtlich relevante Sachverhalte in den Bereichen IT-Sicherheit, Arbeitsverhältnis und E-Commerce gegeben. Ein Exkurs widmet sich letztlich dem Datenschutz in der staatlichen Verwaltung im Bezug auf die wirtschaftliche Nutzung der dort verfügbaren Informationen.

2. Abstract

The present dissertation analyses possible implications arising from the fundamental right of the protection of personal data within corporations in their every day business.

A focus is laid on the mergers and acquisition business, as the acquisition of corporations (as well as shares in those corporations) meanwhile means a common transaction in today's business life. Due to this procedures, legal restructurings of the concerned corporations are almost unavoidable. These restructurings regularly also cause the use of a big amount of personal data.

For the potential purchaser especially important information are usually unfolded in due diligences, thereby it is often a comprehensive providing with personal data, which in the end can be crucial for the success or failure of an acquisition. Analysing the legal circumstances of the use of this personal data is one of the main subjects of the dissertation, a detailed examination is given on the question, whether the universal succession in civil law also results a data protection fact.

Furthermore specific questions in corporate concern structures are examined, as well as an overlook about the category groups IT-security, employer-employee relationship and e-commerce under a data protection point of view is given. The analyses ceases in an excursus concerning data protection in the field of public sector information.

3. Informationen zum Autor

Maximilian Auer, geboren am 22.10.1980 in Rom, Studium der Rechtswissenschaften an den Universitäten Fribourg (CH) und Wien (Mag.iur. 2007).

Teilaspekte der vorliegenden Arbeit wurden gemeinsam mit Dr. Christian Feltl, LL.M. in der Zeitschrift SWK 2009, 815 unter dem Titel „Zur datenschutzrechtlichen Relevanz von Umstrukturierungsvorgängen“ publiziert.