Bundesministerium
des Innern

Modernisierung des Datenschutzrechts

Gutachten im Auftrag des Bundesministeriums des Innern

Alexander Roßnagel

Andreas Pfitzmann

Hansjürgen Garstka

Modernisierung des Datenschutzrechts

Gutachten im Auftrag des Bundesministeriums des Innern

Inhaltsverzeichnis

Abkürzungsverzeichnis

A

a.A.	anderer Ansicht
a.a.O	am angegebenen Ort
AbfG	Abfallgesetz
Abs.	Absatz
ACM	Association for Computing Machinery
AcP	Archiv für civilistische Praxis (Zeitschrift)
a.F.	alte Fassung
AFG	Arbeitsförderungsgesetz
AfP	Archiv für Presserecht (Zeitschrift)
AGB	Allgemeine Geschäftsbedingungen
AGBG	AGB-Gesetz
AK	Arbeitskreis
AK-GG	Alternativkommentar zum Grundgesetz
Anm.	Anmerkung(en)
AO	Abgabenordnung
AöR	Archiv für öffentliches Recht (Zeitschrift)
ArbG	Arbeitsgericht
Art.	Artikel
AsylVfG	Asylverfahrensgesetz
AtG	Atomgesetz
AuslG	Ausländergesetz
AZRG	Gesetz über das Ausländerregister

B

BAG	Bundesarbeitsgericht
BAnz	Bundesanzeiger
BayAbfG	Bayerisches Abfallgesetz
BayDSG	Bayerisches Datenschutzgesetz
BB	Betriebs-Berater (Zeitschrift)
BBB	Council of Better Business Bureaus
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BDSG-E	BDSG-Entwurf
BfD	Bundesbeauftragter für den Datenschutz
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BgrenzSchG	Bundesgrenzschutzgesetz
BImSchG	Bundes-Immisionsschutzgesetz
BK-GG	Bonner Kommentar zum Grundgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtsgesetz
BlnDSG	Berliner Datenschutzgesetz
BMA	Bundesministerium für Arbeit
BMBF	Bundesministerium für Bildung und Forschung
BND	Bundesnachrichtendienst

BR-Drs.	Bundesratsdrucksache
BrDSG	Bremisches Datenschutzgesetz
BRRG	Beamtenrechtsrahmengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drs	Bundestagsdrucksache
BvD	Berufsverband der Datenschutzbeauftragten Deutschland e.V.
BVerfG	Bundesverfassungsgericht
BVerfGE	amtliche Sammlung der Entscheidungen des BVerfG
BverfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BverwGE	amtliche Sammlung der Entscheidungen des BVerwG
BW	Baden-Württemberg

C

CACM	Communications of the ACM (Zeitschrift)
CEPEX	Customer Profile Exchange
CompHdb	Computerhandbuch
COPPA	Children's Online Privacy Protection Act-USA
CPA	Certified Public Accountants
CR	Computer und Recht (Zeitschrift)

D

d.h.	das heißt
DANA	Datenschutznachrichten (Zeitschrift)
DASIT	Projekt: Datenschutz in Telediensten
DB	Der Betrieb (Zeitschrift)
ders.	derselbe
dies.	dieselben
DIN	Deutsche Industrienorm
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSB	Datenschutzbeauftragter
DSG LSA	Sachsen-Anhaltinisches DAtenschutzgesetz
DSG MV	Datenschutzgesetz Macklenburg-Vorpommern
DSG SH	Schleswig-Holsteinisches Datenschutzgesetz
DSRL	EG-Datenschutzrichtlinie 95/46/EG
DSt	Der Staat (Zeitschrift)
DuD	Datenschutz und Datensicherung (Zeitschrift)
DV	Datenverarbeitung
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
DVR	Datenverarbeitung im Recht (Zeitschrift)

E

ECOM	Electronic Commerce Promotion Council of Japan
EEG	Erneuerbare-Energien-Gesetz
EG	Europäische Gemeinschaft(en)
EG-ABl.	Amtsblatt der Europäischen Gemeinschaften
EGAB-Sachs	Erstes Gesetz zur Abfallwirtschaft und zum Bodenschutz im Freistaat Sachsen
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
Einl.	Einleitung

ESRB	Entertainment Software Rating Board

F

f.	folgend(e)
FAQ	frequently asked questions/häufig gestellte Fragen
FernAG	Fernabsatzgesetz
ff.	folgende
Fn.	Fußnote

G

GenTG	Gentechnikgesetz
GewA	Gewerbearchiv (Zeitschrift)
GewArch	Gewerbearchiv (Zeitschrift)
GewO	Gewerbeordnung
GG	Grundgesetz
GK-BimSchG	
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GUID	Globally Unique Identifier
GVBl.	Gesetz- und Verordnungsblatt
GWB	Gesetz gegen Wettbewerbsbeschränkung

H

h.M.	herrschende Meinung
HambAbfG	Hamburgisches Abfallgesetz
HbCompR	Computerrechts-Handbuch, *W. Kilian / B. Heussen* (Hrsg.),
HB-Datenschutzrecht	Handbuch des Datenschutzrechts, *A. Roßnagel*, (Hrsg.),
HDSG	Hessisches Datenschutzgesetz
HPflG	Haftpflichtgesetz
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherehit und Ordnung

I

i.E.	
i.S.d.	im Sinn des
i.V.m.	in Verbindung mit
IFG	Informationsfreiheitsgesetz
IHK	Industrie- und Handelskammer
inkl.	inklusive
insb.	Insbesondere
IP-Adressen	Internet Protocol
ISO	International Standards for Quality Assurance
IT	Informationstechnik
IuKDG	Informations- und Komunikationsdienste-Gesetz

J

JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)

K

Kap.	Kapitel
KJ	Kritische Justiz (Zeitschrift)

KOM	Kommentar
KORA	Konkretisierung rechtlicher Anforderungen
KRG	Krebsregistergesetz
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (Zeitschrift)
KrW-/AbfG	Kreislaufwirtschaft- und Abfallgesetz
KSchG	Kündigungsschutzgesetz
K&R	Kommunikation & Recht (Zeitschrift)

L

LAbfG	Landesabfallgesetz(e)
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LAG	Landesarbeitsgericht
LDSG	Landesdatenschutzgesetz(e)
LDSG BW	Landesdatenschutzgesetz Baden-Württemberg
LDSG Rh.-Pf.	Landesdatenschutzgesetz Rheinland-Pfalz
LDSG SH	Landesdatenschutzgesetz Schleswig-Holstein
LG	Landgericht
LT-Drs.	Landtagsdrucksache
LuftVG	Luftverkehrsgesetz

M

m.w.N.	mit weiteren Nachweisen
MDR	Monatsschirft für Deutsches Recht (Zeitschrift)
MDStV	Mediendienstestaatsvertrag
MedR	Medizinrecht (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
MRRG	Melderechtsrahmengesetz
M-V	Mecklenburg-Vorpommern

N

NAbfG	Niedersächsisches Abfallgesetz
NAI	Networking Advertising Initiative
NDSG	Niedersächsisches Datenschutzgesetz
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeits- und Sozialrecht (Zeitschrift)

O

OECD	Organization for Economic Cooperation and Development
OLG	Oberlandesgericht

P

P3P	Platform for Privacy Preferences
PassG	Passgesetz
PbefG	Personenbeförderungsgesetz
PersAuswG	Personalausweisgesetz
provet	Projektgruppe verfassungsverträgliche Technikgestaltung

R

RdA	Recht der Arbeit (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RFID	Radio frequency identification
RFTAG	Radio-Frequency-Tag
RMD	Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag *A. Roßnagel* (Hrsg.)
Rn.	Randnummer
Rh.-Pf.	Rheinland-Pfalz
Rspr.	Rechtsprechung
RStV	Rundfunk-Staatsvertrag

S

S.	siehe
s.o.	siehe oben
s.u.	siehe unten
SächsDSG	Sächsisches Datenschutzgesetz
SchwbG	Schwerbehindertengesetz
SeeAufgG	Seeaufgabengesetz
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein
SigG	Signaturgesetz
sog.	sogenannte(r)
SoldatenG	Soldatengesetz
StGB	Strafgesetzbuch
StörfallV	Störfallverordnung
Stop	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
STVollzG	Strafvollzugsgesetz

T

TB	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDDSG-E	Teledienstedatenschutzgesetz - Entwurf
TDG	Teledienstegesetz
TDSV	Telekommunikationsdiensteunternehmen-Datenschutzverodnung
ThürDSG	Thüringer Datenschutzgesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TPG	Transplantationsgesetz
TVG	Tarifvertragsgesetz

U

u.a.	und andere / unter anderem
UGB	Umweltgesetzbuch
UMTS	Universal Mobile Telecommunications System
UmwHaftG	Umwelt-Haftungsgesetz
UPR	Umwelt- und Planungsrecht (Zeitschrift)
UWG	Gesetz gegen den unlauteren Wettbewerb

V

VersR	Versicherungsrecht (Zeitschrift)
Verw	Die Verwaltung (Zeitschrift)
VG	Verwaltungsgericht
vgl.	vergleiche
VuR	Verbraucher und Recht (Zeitschrift)
VV	Verwaltungsvorschrift
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

W

W3C	World Wide Web Consortium
WHG	Wasserhaushaltsgesetz
WiR	Wirtschaftsrecht (Zeitschrift)
WWW	World Wide Web

X

XML	Extensible Markup Language

Z

z.B.	zum Beispiel
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht (Zeitschrift)
ZivildienstG	Zivildienstgesetz
ZPO	Zivilprozessordnung
ZPR	Zeitschrift für Rechtspolitik (Zeitschrift)

Vorwort

Es ist weltweit anerkannt, dass sich die Informationsgesellschaft als soziales und wirtschaftliches Paradigma der nächsten Jahrzehnte nur entwickeln kann, wenn hinreichende rechtsstaatliche Sicherungen einen hohen Standard der Persönlichkeitsrechte gewährleisten. Diese Funktion wurde seit den 60er Jahren in den Industrienationen, zunehmend aber auch in vielen anderen Staaten vorrangig der Datenschutzgesetzgebung zugewiesen. Ihr verfassungsrechtlicher Stellenwert wird inzwischen auf nationalstaatlicher Ebene in Verfassungen und Verfassungsrechtsprechung, in der Europäischen Grundrechtecharta und auch in der UNO-Resolution vom Dezember 1990 anerkannt.

In Deutschland wurde nach den bahnbrechenden Gesetzen der Länder Hessen und Rheinland-Pfalz am 27. Januar 1977 das erste Bundesdatenschutzgesetz geschaffen, dem Regelungen in allen Bundesländern folgten. Das deutsche Datenschutzrecht musste in Folge des Volkszählungsurteils von 1983 jedenfalls im öffentlichen Bereich deutliche Änderungen erfahren.

Mit der europäischen Datenschutzrichtlinie von 1995 entstand darüber hinaus ein weiterer Änderungsbedarf, der von der deutschen Bundesregierung zunächst als eher zu vernachlässigend eingeschätzt, im Verlauf der Jahre jedoch ernster genommen wurde, ohne dass allerdings bis zum Ende der 13. Legislaturperiode des Bundestages ein Gesetz verabschiedet worden wäre, das die Vorgaben dieser Richtlinie umsetzte.

Die neue Bundesregierung sah sich in der Situation, dass nahezu zeitgleich mit ihrem Regierungsantritt die Umsetzungsfrist der Richtlinie abgelaufen war. Trotz der nunmehr vorhandenen Einsicht, dass die zuvor von vielen Fachkreisen geäußerte Meinung richtig ist, die vorliegenden Arbeitspapiere der Bundesregierung würden die Richtlinie nicht hinreichend umsetzen und seien zu wenig zukunftsweisend, machte es die drohende Klage der europäischen Kommission vor dem Europäischen Gerichtshof erforderlich, auf der Basis der vorhandenen Vorentwürfe einen Novellierungsentwurf zum Bundesdatenschutzgesetz vorzulegen. Das nunmehr dritte BDSG (BDSG 2001) trat am 23. Mai 2001 in Kraft.

Die Bundesregierung und die Koalitionsfraktionen waren sich bei dieser Vorgehensweise bewusst, dass ein modernes Datenschutzrecht nur durch eine grundsätzliche Neugestaltung geschaffen werden kann, die auch die Grundstrukturen des Gesetzes umfassen muss. Der Gesetzentwurf eines neuen BDSG der Fraktion Bündnis 90/DIE GRÜNEN aus dem Jahre 1997 beinhaltete bereits grundsätzliche Neuerungen – neben den zur Umsetzung der europäischen Datenschutzrichtlinie notwendigen Regelungen. Eckwerte für eine Neugestaltung waren auch von der SPD Bundestagsfraktion bereits im Jahr 1998 vorgelegt worden. Die Unübersichtlichkeit der bestehenden datenschutzrechtlichen Regelungen – sowohl des Datenschutzgesetzes selbst als auch der Vielzahl an bereichsspezifischen Regelungen –, die Nichtberücksichtigung moderner technischer Entwicklungen, mangelhafte Umsetzung der Europäischen Datenschutzrichtlinie und die sich aus der Internationalisierung und Globalisierung ergebenden Anforderungen wurden als Hauptgründe für den Erneuerungsbedarf benannt.

Schon bald nach dem Regierungswechsel fanden erste Gespräche über die Vorgehensweise statt. Sie führten zu dem Ergebnis, dass parallel zum Gesetzgebungsverfahren des BDSG 2001 als erster Schritt einer zweiten Stufe zur Modernisierung des Datenschutzrechts ein Gutachten über deren grundsätzliche Problemstellungen eingeholt werden sollte, das als Ausgangsbasis für die Ausformulierung eines neuen Gesetzes dienen kann.

Das Bundesministerium des Innern beauftragte daraufhin die Professoren Dr. Alexander Roßnagel, Universität Kassel, und Dr. Andreas Pfitzmann, Technische Universität Dresden, ein Gutachten zum Thema: „Modernisierung des Datenschutzrechts, insbesondere grundlegende Novellierung des Bundesdatenschutzgesetzes“ zu erstellen. Die Hinzuziehung eines Hochschullehrers für Informatik sollte den Stellenwert markieren, den technische Regelungen

künftig im Datenschutzrecht haben sollten. Mit der Koordinierung des Projektes wurde der Berliner Beauftragte für Datenschutz und Akteneinsicht, Prof. Dr. Hansjürgen Garstka beauftragt und ihm mit David Gill ein Referent zur Seite gestellt, der das Projekt während seiner Laufzeit betreute. Der wissenschaftliche Mitarbeiter Philip Scholz sowie Dipl.-Inform. Marit Köhntopp unterstützten die Arbeiten.

Von Anfang an war beabsichtigt, das Gutachten nicht im Alleingang zu erstellen, sondern in mehreren Stufen möglichst weit gefächerten Sachverstand in die Arbeit einzubeziehen. Die Koalitionsfraktionen unterstützten das Projekt zum einen durch die initiale Veranstaltung eines Workshops vom 15.-18. Juni 2000, in dem eine Reihe in- und ausländischer Experten grundlegende Gedanken zur Modernisierung des Datenschutzrechts vortrugen. Die Beratung der Gutachter wurde zum anderen durch eine Begleitkommission wahrgenommen, der ein repräsentativer Querschnitt der deutschen Datenschutzexperten angehörte, die in den Sitzungen am 15. Januar und 25. Juni 2001 die Zwischenergebnisse des Projektes diskutierten.

Vom Bundesministerium des Innern unterstützt wurde die Durchführung von Workshops mit Vertretern einzelner Interessenbereiche („Fachgespräche"). Derartige Sitzungen fanden statt

- am 23. Februar 2001 mit dem Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik,
- am 5. März 2001 mit dem Arbeitskreis „Datenschutz" der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. sowie der Gesellschaft für Datenschutz und Datensicherung, die die Interessen der Wirtschaft und der betrieblichen Datenschutzbeauftragten vertraten,
- am 14. März 2001 mit Vertretern von Verbraucher-, Berufs- und Datenschutzverbänden, Informatikvereinen und Experten im Arbeitnehmerdatenschutz,
- am 2. April 2001 mit Experten des Bundesamtes für die Sicherheit in der Informationstechnik,
- am 3. April 2001 mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Weitere Gespräche wurden am 16. Mai 2001 mit Fachabteilungen des Bundesministeriums des Innern sowie am 12. Juli 2001 mit dem Arbeitskreis II der Innenministerkonferenz geführt.

Die Anregungen und Vorschläge aus der Begleitkommission, den Fachgesprächen und sonstigen Gesprächen sind im Anhang zusammengefasst.

Die Arbeitsergebnisse wurden in mehreren Arbeitsbesprechungen der Gutachter sowie einer Klausursitzung am 20.-22. Mai 2001 in Bischofsheim/Rhön beraten.

Das nunmehr vorliegende Gutachten wurde von Alexander Roßnagel in seiner Grundstruktur konzipiert und ausgeführt. Andreas Pfitzmann steuerte das erforderliche informatische Fachwissen bei. Die Ausführungen zur Kontrolle des Datenschutzes wurden von David Gill gefertigt.

Für das Gutachten stehen die strukturellen Änderungen des Datenschutzrechts im Vordergrund – wie etwa die Möglichkeiten, das Datenschutzrecht zu vereinfachen sowie klarer und verständlicher zu regeln, die Selbstbestimmung der betroffenen Person und die Selbstregulierung der verantwortlichen Stellen zu stärken, Datenschutz besser auf die künftigen Risiken der informationstechnischen Entwicklung einzustellen, sowie neue Instrumente einzuführen, die bisher vernachlässigte Kräfte für die Umsetzung von Datenschutz aktivieren. Einzelne Detailregelungen, sofern sie nicht für die neuen Strukturen tragend waren, wurden nicht als vorrangige Aufgabe gesehen. So wurde zum Beispiel auf die Erörterung der Regelungen zur

Datenübermittlung in andere Staaten verzichtet, die gerade im BDSG 2001 aufgenommen wurden und die Bestimmungen der Europäischen Datenschutzrichtlinie mehr oder weniger direkt übernehmen. Spezifische Datenschutzregelungen in den einzelnen Fachbereichen der öffentlichen Verwaltung, insbesondere im Sicherheitsbereich, konnten angesichts der Kürze der zur Verfügung stehenden Zeit nicht behandelt werden, wenngleich sowohl die Auswirkungen der Neukonzeption auf das Verhältnis von allgemeinem und bereichsspezifischem Datenschutzrecht als auch die absehbaren Folgen neuer Datenschutzkonzepte auf die Aufgabenerfüllung der Verwaltungsbehörden berücksichtigt werden. Das Verhältnis des Datenschutzes zur Informationsfreiheit war trotz seiner aktuellen Brisanz nicht Gegenstand des Auftrags. Die Vorschläge sind überdies so gehalten, dass eine Änderung des Grundgesetzes vermieden werden kann, obwohl es hierzu zum Beispiel im Bereich des Mediendatenschutzes Überlegungen gibt.

Das Gutachten enthält zur Verdeutlichung auch Ausführungen und Vorschläge für einzelne Regelungen. Für ihre Ausgestaltung wurden bisweilen auch mehrere Möglichkeiten angedeutet. In den beispielhaften Vorschlägen zu einzelnen Gesetzesvorschriften sind dann allerdings die Regelungen gewählt, die den Gutachtern am sinnvollsten erscheinen. Dies schließt nicht aus, im Detail andere Ausgestaltungen zu wählen, soweit sie nicht das vorgeschlagene Gesamtsystem gefährden.

Die Modernisierung des Datenschutzrechts wird nach der Novellierung des Bundesdatenschutzgesetzes selbst in einem weiteren Schritt die umfängliche Umsetzung der allgemeinen Regeln in den bereichspezifischen Datenschutzgesetzen nach sich ziehen. Dies ist Anliegen des Gesamtvorhabens, das sich an einer generellen Vereinfachung und Verschlankung orientiert und liegt somit in der Natur der Sache. Zur Neuregelung oder auch völligen Aufhebung bereichsspezifischer Gesetze schlägt das Gutachten ehrgeizige Übergangsfristen vor. Den Gutachtern ist bewusst, dass diese Fristen letztlich von praktischen Vorgaben abhängen. Gleichwohl verstehen sie ihre Vorschläge als Ermunterung für eine schnelle Umsetzung auch in diesem Bereich.

Es ist offenkundig, dass die erfolgreiche Umsetzung der vorgelegten Vorschläge nicht ohne entsprechende gesetzgeberische Maßnahmen in den Ländern vorgenommen werden kann. Im Arbeitskreis II der Innenministerkonferenz wurde daher angeregt, auf der Grundlage des vorliegenden Gutachtens entsprechende Beratungen mit den Ländern aufzunehmen.

Die vorgelegten Vorschläge versuchen, sich innerhalb der Regulierungsbandbreite der Europäischen Datenschutzrichtlinie zu halten. Gleichwohl sollten die dargelegten Gesichtspunkte auch in die Fortentwicklung des europäischen Rahmenwerkes einfließen.

Der Dank des Gutachterausschusses gilt den Fraktionen der SPD und BÜNDNIS 90 / DIE GRÜNEN des Bundestages und ihren Mitarbeitern sowie dem Datenschutzfachreferat des Bundesministeriums des Innern für die vorzügliche Zusammenarbeit.

Ergebniszusammenfassung in Thesen

1. Datenschutz ist Grundrechtsschutz und Funktionsbedingung eines demokratischen Gemeinwesens. Er ist notwendiger Bestandteil einer freiheitlichen Kommunikationsordnung. Teilhabe und Teilnahme an demokratischer Willensbildung und einem freien Wirtschaftsverkehr sind nur zu erwarten, wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann. Diese ist nur möglich, wenn die Erhebung und Verwendung von Daten über ihn grundsätzlich seiner freien Selbstbestimmung unterliegt.

Datenschutz ist ein wichtiger Akzeptanzfaktor der Informationsgesellschaft. Seine rechtliche Gestaltung beeinflusst die Entwicklung einer modernen Wirtschaft. Er ist der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

2. Diesen Grundsätzen trägt das bisherige Datenschutzrecht in Deutschland nur bedingt Rechnung. Es ist immer noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert, nimmt neue Formen personenbezogener Daten und deren Verarbeitung nur ungenügend auf und berücksichtigt unzureichend die Gefahren und Chancen neuer Techniken der Datenverarbeitung. Darüber hinaus ist es in seinen Formulierungen häufig widersprüchlich und durch seine Normierung in hunderten von speziellen Gesetzen unübersichtlich und schwer zu handhaben.

3. Die positiven Erwartungen an das Datenschutzrecht und die Unzulänglichkeit der bisherigen Regelungen aufnehmend, soll ein modernes Datenschutzrecht geschaffen werden, das zum Einen einfacher und verständlicher und zum Anderen angesichts neuer Formen der Datenverarbeitung risikoadäquat ist. Um das erste Ziel zu erreichen, müssen die Selbstbestimmung der betroffenen Person gestärkt und die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden. Um das zweite Ziel zu erreichen, müssen vor allem Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt werden.

Ein allgemeines Gesetz - nur wenige Spezialregelungen

4. Ein modernes Datenschutzrecht sollte auf einem *allgemeinen Gesetz* gründen, das bereichsspezifischen Regelungen vorgeht. Dieses enthält grundsätzliche und präzise Regelungen der Verarbeitung personenbezogener Daten und vermeidet möglichst offene Abwägungsklauseln. Das Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten. Wird die Vorrangregelung im Verhältnis zwischen BDSG und bereichsspezifischen Regelungen umgedreht, können die bisherige Normenflut und Rechtszersplitterung verringert und Widersprüche vermieden werden.

5. *Spezialregelungen* in bereichsspezifischen Gesetzen sollten nur Ausnahmen von den allgemeinen Regelungen enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten. Auch könnten Ausnahmen vorgesehen werden, wenn Aufgaben im Allgemeininteresse ansonsten nicht erfüllt werden können. Alle Ausnahmen sind als explizite Durchbrechungen der allgemeinen Prinzipien durch Formulierungen wie „... in Abweichung von § X BDSG ...“ kenntlich zu machen.

6. Das *Telekommunikations-* (§§ 85 und 89 TKG und TDSV) und *Teledienstedatenschutzrecht* (TDDSG) sollten *in das BDSG integriert* werden. Dies entspricht der Bedeutung der Telekommunikation für die Verarbeitung personenbezogener Daten. Dadurch könnten Wertungswidersprüche und Überschneidungen der Anwendungsbereiche beseitigt und eine Vereinheitlichung auf hohem Niveau erreicht werden.

7. *Schutzgut* des Datenschutzrechts ist die informationelle Selbstbestimmung, die das Bundesverfassungsgericht als risikoorientierte Ausprägung der Grundrechte in der Informationsgesellschaft entwickelt hat.

8. Die allgemeinen *Datenschutzgrundsätze* sollten *gleichermaßen für den öffentlichen und für den nicht öffentlichen Bereich* gelten. In beiden Bereichen ist – risiko- und nicht bereichsabhängig – das gleiche Datenschutzniveau zu gewährleisten. Unterschiede sind insoweit zu berücksichtigen, als im nicht öffentlichen Bereich die Regelungsadressaten Grundrechtsträger sind und im öffentlichen Bereich Allgemeininteressen verfolgt werden müssen.

9. Die Grundsätze sollten *nicht zwischen manueller und automatischer Datenverarbeitung unterscheiden*. Die Unterscheidung zwischen Dateien und Akten beschreibt nicht die Grenze zwischen erforderlichem Schutz und irrelevanten Verhaltensweisen und führt zu unsachlichen Abgrenzungen. Soweit zweckmäßig können einzelne Pflichten auf Dateien oder die automatisierte Datenverarbeitung beschränkt werden.

10. *Juristische Personen* sollten in den Schutzbereich des Datenschutzrechts einbezogen werden. Das Grundrecht auf informationelle Selbstbestimmung gilt, soweit nicht gerade sein persönlichkeitsrechtlicher Kern betroffen ist, nach Art. 19 Abs. 3 GG auch für juristische Personen. Auch das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG gilt nach Art. 19 Abs. 3 GG für juristische Personen. Daher erstreckt das Telekommunikations-Datenschutzrecht bereits heute seinen Schutz auch auf juristische Personen. Wenn künftig Telekommunikation ein Regelbestandteil der Datenverarbeitung wird und das Telekommunikations-Datenschutzrecht in das BDSG integriert werden soll, können dessen Regelungen weder auf natürliche Personen beschränkt werden, noch kann der personelle Schutzbereich für die Datenverarbeitung in und außerhalb der Telekommunikation unterschiedlich bestimmt werden. Darüber hinaus ist die Abgrenzung zwischen Daten natürlicher und juristischer Personen in der Aufsichtstätigkeit ohnehin häufig schwierig oder unmöglich. Dateien über juristische Personen enthalten in der Regel auch Daten zu natürlichen Personen. Daher werden die Daten in der Praxis grundsätzlich ohne weitere Differenzierung dem höheren Schutzniveau unterstellt. Die Einbeziehung juristischer Personen wäre somit auch praxisadäquat.

Grundsätze der Datenverarbeitung

11. Datenschutz soll künftig vorrangig durch Grundsätze der Datenverarbeitung erfolgen, die einerseits ein Mindestschutzniveau beschreiben und andererseits der betroffenen Person Kontroll- und Mitwirkungsmöglichkeiten bieten. Daneben kann aber aus europa- und verfassungsrechtlichen Gründen auf gesetzliche Erlaubnisse der Datenverarbeitung nicht verzichtet werden. Diese sollen jedoch erheblich vereinfacht werden.

12. Jeder Umgang mit personenbezogenen Daten sollte unter einer *einheitlichen Bezeichnung* erfasst werden. Entsprechend der Europäischen Datenschutzrichtlinie bietet sich die Bezeichnung der „*Verarbeitung*“ an. Nicht alle Formen der Datenverarbeitung werden künftig jedoch nach den gleichen Regeln behandelt werden können. Um insbesondere die Datenverarbeitung für das Erbringen technischer Leistungen adäquat regeln zu können, sollte das künftige Datenschutzrecht zwischen *zwei Kategorien der Datenverarbeitung* unterscheiden:

- *Verarbeitung mit gezieltem Personenbezug* zum Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Personalakten, Vertragsdaten, Bestandsdaten) und
- *Verarbeitung ohne gezielten Personenbezug* zu anderen Zwecken als dem Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Erbringen technischer Dienstleistungen, Kommunikation von Maschine zu Maschine, „Überschussdaten“ bei Suchprozessen)

Die *Datenverarbeitung ohne gezielten Personenbezug* betrifft die bereits heute gewaltige Menge von Daten, die für technische Dienstleistungen der Telekommunikation verarbeitet werden muss. Diese wird vervielfacht durch das technische Ermöglichen, im Cyberspace zu handeln. Sie wird potenziert, wenn die unübersehbare Vielfalt des Ubiquitous Computing in der Alltagswelt hinzu kommt.

Die Anforderungen für die Verarbeitung ohne gezielten Personenbezug sollten risikoadäquat und effizienzsteigernd spezifiziert werden. Sie werden insofern verschärft, als die Daten auf das erforderliche Minimum begrenzt, während ihrer Verarbeitung gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden müssen. Die Daten sollten außerdem einer strengen Zweckbindung (wie nach § 31 BDSG) unterliegen und durch ein Verwertungsverbot geschützt sein. Werden diese Anforderungen nicht erfüllt, wird vor allem ein weitergehender Zweck mit diesen Daten verfolgt, gelten für sie von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug. Erleichterungen sollten insoweit vorgesehen werden, als auf eine vorherige Unterrichtung der betroffenen Personen verzichtet wird und ein Anspruch auf Auskunft über einzelne Daten für die kurze Zeit ihrer Speicherung nicht besteht. Ein solcher Anspruch erscheint kontraproduktiv. Er hätte den unerwünschten Effekt, dass Protokollverfahren oder Data-Mining-Techniken nur deshalb angewendet werden müssten, um die personenbezogenen Daten ausfindig zu machen und zusammenzuführen. Die notwendige Transparenz soll durch eine öffentliche und allgemeine Datenschutzerklärung des Datenverarbeiters über die Struktur seines Datenverarbeitungsverfahrens hergestellt werden.

Hohe Transparenz der Datenverarbeitung

13. Wenn das Datenschutzrecht entlastet und die Regelung des Datenverarbeitungsverhältnisses stärker seinen beiden Parteien überlassen werden soll, muss die Transparenz der Datenverarbeitung gegenüber der betroffenen Person erhöht werden. Zielsetzung eines modernen Datenschutzrechts muss es sein, ausreichende Informationen über die Erhebung personenbezogener Daten, über die Umstände und Verfahren ihrer Verarbeitung und die Zwecke ihrer Nutzung für die betroffenen Personen und die Kontrollstellen sicherzustellen. Wer geschäftsmäßig personenbezogene Daten automatisiert verarbeitet, sollte verpflichtet sein, die Struktur der Datenverarbeitung in verständlicher Form zu veröffentlichen, soweit dies ohne Offenlegung von schützenswerten Geheimnissen möglich ist. Mit angemessenem Aufwand muss überdies durchschaubar sein, was das System einschließlich aller Betriebs- und Anwendungssoftware genau tut.

Stärkung der Selbstbestimmung

14. Obwohl in die Informationsgesellschaft kein formelles Verbot der Datenverarbeitung passt, muss dennoch aus verfassungs- und europarechtlichen Gründen die Datenverarbeitung jeweils spezifisch erlaubt werden. Um Datenschutz zu vereinfachen und absurde Ergebnisse zu vermeiden, sollte ein *genereller Erlaubnistatbestand* die Datenverarbeitung immer dann für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Person zu erwarten ist.

15. Soweit die Datenverarbeitung Interessen der betroffenen Person beeinträchtigen könnte, soll die Entscheidung über diese vorrangig der *Selbstbestimmung der betroffenen Person* überlassen werden. Im Einzelfall muss die Datenverarbeitung grundsätzlich durch *Einwilligung* oder Einwilligungssurrogate wie Vertrag und vertragsähnliches Vertrauensverhältnis oder Antrag gegenüber einer Behörde erlaubt werden können. Die Einwilligung ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung. Da aber zwischen den betroffenen Personen und den verantwortlichen Stellen in der Regel ein erhebliches Machtgefälle besteht, muss die Selbstbestimmung gestärkt werden. Ziel eines modernen Datenschutzrechts muss es daher sein, einerseits die Zulässigkeit der Datenverarbeitung im vertretbaren Umfang

der individuellen Selbstbestimmung zu überlassen, andererseits aber deren Freiwilligkeit durch Rahmenregelungen abzusichern.

16. Grundsätzlich sollte im *nicht öffentlichen Bereich* eine „Opt-in-Lösung“ gewählt werden: Die Datenverarbeitung setzt die vorherige Einwilligung der betroffenen Person voraus. Allerdings muss eine Datenverarbeitung auch ohne Einwilligung der betroffenen Person möglich sein. Zur Umschreibung dieser Ausnahmefälle ist der bisher die Datenverarbeitung steuernde Begriff des „berechtigten Interesses“ zu weit. Ausnahmen sollten nur erlaubt sein, wenn dies zum Schutz oder zur Verfolgung eigener Rechte oder Rechte Dritter notwendig ist, oder wenn es erforderlich ist, um eine Gefahr für Leben, Gesundheit oder sonstige bedeutende Rechtsgüter der betroffenen Person zu beseitigen, und die betroffene Person ihre Zustimmung nicht geben kann, oder wenn die Datenverarbeitung erforderlich ist, um Verpflichtungen zu erfüllen, die durch Rechtsvorschriften der verantwortlichen Stelle auferlegt wurden.

17. Im *öffentlichen* Bereich sollte die Datenverarbeitung zulässig sein, wenn sie „zur Erfüllung einer gesetzlich zugewiesenen und in der Zuständigkeit der öffentlichen Stelle liegenden bestimmten Aufgabe erforderlich“ ist. Soweit es allerdings um Verarbeitungszwecke und -formen geht, die gegen den Willen der betroffenen Person durchgesetzt werden müssen und deren Interessen stark beeinträchtigen können, sollen bereichsspezifische Regelungen die Zwecke und Formen risikoadäquat regeln. Die Einwilligung kann im öffentlichen Bereich die Datenverarbeitung im Wesentlichen nur im nicht gesetzlich gebundenen Bereich legitimieren.

Erforderlichkeit der Datenverarbeitung und Vermeidung des Personenbezugs

18. Soweit für die Zwecke der Datenverarbeitung ein Personenbezug nicht erforderlich ist, muss dieser von Anfang an vermieden oder nachträglich durch Löschung der Daten, ihre Anonymisierung oder Pseudonymisierung beseitigt werden. Darüber hinaus sind die verantwortlichen Stellen zu verpflichten, soweit dies technisch möglich und verhältnismäßig ist, ihre Datenverarbeitungsverfahren so zu gestalten, dass sie möglichst keinen Personenbezug und auch keine Personenbeziehbarkeit aufweisen. Dieses Ziel kann durch *Anonymität* oder *Pseudonymität* der betroffenen Person erreicht werden. Anonymität und anonymitätsnahen Arten von Pseudonymen sollte grundsätzlich Vorrang gegeben werden.

19. Die vorgenannten Grundsätze der Transparenz und der Vermeidung des Personenbezugs können nur durch die betroffenen Personen selbst durchgesetzt werden (*Selbstdatenschutz*). Sie müssen in die Lage versetzt werden, die Nutzung von technischen und organisatorischen Schutzinstrumenten selbst zu bestimmen. Dies sind Instrumente für Inhaltsschutz (Konzelation, Steganographie), Anonymität, Pseudonymität und Identitätsmanagement. Programme, die Schlüssel, Identitäten und Pseudonyme verwalten und den Nutzer bei der Verwendung von Selbstschutztechniken unterstützen, müssen gefördert werden. Eine Bildungsoffensive zum Umgang mit Instrumenten des Selbstdatenschutzes wäre zu erwägen.

Zweckbegrenzung und Zweckbindung der Datenverarbeitung

20. Die *Zweckbindung* bestimmt Ziel und Umfang zulässiger Datenverarbeitung und begrenzt sie zugleich auf diese. Eine Verarbeitung personenbezogener Daten darf nur zu bestimmten, in der Einwilligung oder der gesetzlichen Erlaubnis ausdrücklich genannten Zwecken erfolgen. *Systemdatenschutz* kann die technisch-organisatorische Sicherung der Zweckbindung unterstützen: Grundsätzlich sollten die verwendeten Produkte und die eingerichteten Datenverarbeitungsprozesse für die verarbeitenden Personen nur die Maßnahmen zulassen, die dem Zweck der Datenverarbeitung entsprechen.

21. *Profilbildungen* sind eine besondere Gefahr für die informationelle Selbstbestimmung. Gleichwohl sollten sie nicht generell verboten werden. Eine Kombination von Anforderungen könnte den erforderlichen Schutz bieten, wenn dadurch vor allem Transparenz und Einflussnahme für die betroffene Person gewährleistet sind. So ist die beabsichtigte Profilbildung als

spezifische Form der Datenverarbeitung in der Datenschutzerklärung mit einem Hinweis auf ihre Struktur und ihren Zweck darzustellen. Grundsätzlich muss die Profilbildung von einer ausdrückliche Einwilligung gedeckt sein und die betroffene Person jederzeit die Möglichkeit haben, ihre Einwilligung für die Zukunft zu widerrufen. Nur in Ausnahmefällen sollte die Profilbildung durch einen Erlaubnistatbestand legitimiert werden, was allerdings die Unterrichtung und ein Widerspruchsrecht der betroffenen Person voraussetzt.

Organisatorische Unterstützung der Grundsätze der Datenverarbeitung

22. Viele bereits bestehende organisatorische Verpflichtungen der verantwortlichen Stellen sollten zu einem integrierten *Datenschutzmanagementsystem* zusammengefasst und fortentwickelt werden, um Verantwortlichkeit sicher zu stellen, das Datenschutzbewusstsein zu stärken und eine datenschutzfreundliche Betriebsorganisation zu erreichen. Die Bestellung eines Datenschutzbeauftragten, die Erarbeitung eines Plans der Datenschutzorganisation und die Erstellung eines Datenschutz- und Datensicherungskonzepts sind die wesentlichen Bestandteile.

23. Zur Stärkung der Akzeptanz des Datenschutzes und um eine ständige Fortentwicklung entsprechend den sich verändernden und zunehmenden Risiken zu ermöglichen, muss ein modernes Datenschutzrecht auch *Anreize* für einen effektiven und sich fortentwickelnden Schutz bieten. Daher wird den verantwortlichen Stellen die Möglichkeit geboten, mit ihren Anstrengungen zur Implementierung eines effektiven Datenschutzes zu werben. Hierzu gehören insbesondere die vertrauenswürdige Auditierung von Datenschutzmanagementsystemen, die mit Erleichterungen rechtlicher Anforderungen belohnt werden sollte. Verantwortliche Stellen, die am *Datenschutzaudit* teilnehmen, sollten von öffentlichen Stellen außerdem bevorzugt berücksichtigt werden, wenn es um Aufträge zur Verarbeitung personenbezogener Daten geht.

Mit dem Datenschutzaudit könnte unabhängig von der Novellierung des BDSG noch in dieser Legislaturperiode ein erster Schritt der zweiten Novellierungsstufe realisiert werden.

Datenschutz durch Technik

24. Datenschutz muss künftig durch, nicht gegen *Technik* erreicht werden. Datenschutzrecht muss versuchen, die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes auszurichten und die Diffusion und Nutzung datenschutzgerechter oder -fördernder Technik zu fördern. Datenschutz sollte so weit wie möglich in Produkte, Dienste und Verfahren integriert sein. Adressaten des Datenschutzrechts können daher nicht mehr nur die für die Datenverarbeitung verantwortlichen Stellen sein. Das Datenschutzrecht muss bereits bei der Entwicklung der Technik Einfluss auf deren Gestaltung nehmen. Es muss *datenschutzgerechte Technik fordern und fördern*. Zu diesem Zweck sollten zumindest drei Regelungen vorgesehen werden. Die Hersteller sollten verpflichtetet werden, für die Gestaltung ihrer Produkte zumindest die Erfüllung einiger zentraler Produktanforderungen zu überprüfen. Wer datenschutzgerechte Produkte herstellt, sollte die Möglichkeit erhalten, diese zertifizieren zu lassen und mit dem Zertifikat werben zu können. Schließlich sollten die verantwortlichen Stellen aufgefordert werden, datenschutzgerechte Produkte zu verwenden. Zumindest für öffentliche Stellen sollte dies zu einer gesetzlichen Pflicht erhoben werden.

Gesellschaftliche Selbstregulierung

25. Konkretisierungen der gesetzlichen Grundsätze können durch branchen- oder unternehmensspezifische *Selbstregulierung* erfolgen. Um in dieser ein faires Verfahren, einen angemessenen Interessenausgleich, die Berücksichtigung von Gemeinwohlinteressen und eine gewisse demokratische Legitimation zu gewährleisten, muss der Gesetzgeber auch für diese Regelsetzung einen gesetzlichen Rahmen vorgeben. Selbstregulierung ermöglicht es der Wirtschaft, relativ schnell passgerechte branchen- oder unternehmensbezogene verbindliche Rege-

lungen zu entwickeln, die die schnelle Entwicklung der Technik, die Komplexität ihrer Systeme und die Vielfalt ihrer Anwendungen berücksichtigen. Der entscheidende Anreiz für Branchen, Verbände oder Unternehmen, eigene, durch Kontrollstellen anerkannte Verhaltensregeln zu erstellen, besteht in der Möglichkeit, die zu konkretisierenden Gesetzesvorgaben selbständig und auch für die Kontrollstellen verbindlich auszugestalten.

26. Die Selbstregulierung könnte *beispielsweise* Konkretisierungen der Erlaubnistatbestände „Verfolgung und Schutz eigener Rechte oder Rechte Dritter“ sowie der Erforderlichkeit bestimmter Daten für bestimmte Zwecke zum Inhalt haben. Andere Beispiele wären die brancheneinheitliche Festlegung notwendiger Vertragsdaten, von Grundsätzen für die branchenspezifische Unterrichtung betroffener Personen oder von branchenspezifischen Datenschutzerklärungen. Ebenso könnten Verfahren anonymen und pseudonymen Handelns festgelegt oder die Einrichtung branchenspezifischer Schlichtungsverfahren vorgesehen werden. Schließlich wäre an die Erarbeitung einheitlicher Einwilligungserklärungen zu denken.

27. Die Selbstregulierung sollte auf einen gesellschaftlichen Konsens, nicht auf die einseitige Durchsetzung der Interessen eines Verbands zielen. Daher sollten sich anerkannte Datenschutz- und Verbraucherverbände an der Selbstregulierung beteiligen können.

28. In diesem Zusammenhang sollte das Gesetz der Bundesregierung die Möglichkeit bieten, für die freiwillige Erfüllung von Anforderungen zur Vorsorge gegen Risiken für die informationelle Selbstbestimmung formell *Zielfestlegungen* zu treffen, die innerhalb einer bestimmten Frist erreicht werden sollen. Diese ermöglichen es, Prioritäten zu setzen und die Richtung der Politik zu bestimmen. Die Zielfestlegung wirkt entweder normvermeidend, wenn die Ziele freiwillig erfüllt werden oder sie wirkt normvorbereitend, indem sie die künftigen Regelungsadressaten bereits auf die Regelung „einstimmt“. Nach Ablauf der vorgegebenen Frist wäre zu prüfen, ob und welche gesetzgeberischen Maßnahmen zu ergreifen sind.

Stärkung der Betroffenenrechte

29. *Betroffenenrechte* bieten eine wesentliche Stütze für einen effektiven Datenschutz nur, wenn sie von den Betroffenen auch tatsächlich wahrgenommen werden und wahrgenommen werden können. Die betroffenen Personen müssen ihre Rechte frei und unbehindert sowie unentgeltlich ausüben können, ohne Zwang, dies zu tun oder nicht zu tun. Betroffenenrechte sollten wenn möglich nur im allgemeinen Datenschutzgesetz geregelt und möglichst knapp und einfach formuliert werden, damit auch die Betroffenen selbst sie verstehen. Sie sind ausdrücklich für unabdingbar zu erklären und dürfen nicht durch Rechtsgeschäft ausgeschlossen werden können. Die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen ist auch bezüglich der Betroffenenrechte aufzugeben. Im Rahmen der Online-Kommunikation sollten die betroffenen Personen ihre Rechte auch telekommunikativ wahrnehmen können. Die betroffene Person sollte bereits vor der Datenerhebung über ihre Rechte informiert werden. Die Informations- und Unterrichtungspflichten sind daher entsprechend auszuweiten.

30. Die *Auskunft* sollte umfassend erfolgen und sich je nach Anforderung der betroffenen Person auf alle Aspekte der Datenverarbeitung erstrecken. Insbesondere gehören hierzu Angaben zu den gespeicherten Daten selbst, zu deren Herkunft, zu den Empfängern der Daten und Teilnehmern eines automatisierten Abrufverfahrens, zum Zweck der Datenverarbeitung, zum Auftragnehmer bei Datenverarbeitung im Auftrag und zum Dienstleister bei Outsourcing, wie auch Angaben über die erfolgte Berichtigung, Löschung oder Sperrung von Daten, über den Aufbau, die Struktur und den Ablauf der automatisierten Datenverarbeitung, insbesondere über Profilbildungen und deren Struktur. Ausnahmen von der Auskunftspflicht sollten auf wenige unabdingbaren Fallkonstellationen reduziert werden.

31. Jede betroffene Person kann den betrieblichen oder behördlichen Datenschutzbeauftragten als *Beschwerdeinstanz* anrufen. Er soll auf eine gütliche Lösung zwischen der verantwortlichen Stelle und der betroffenen Person hinwirken und innerhalb eines Monats eine schriftliche und mit Gründen versehene Antwort auf die Beschwerde abgeben.

32. Der betroffenen Person sollte ein Recht zum Widerspruch, wie es auch von Art. 14 a) DSRL gefordert wird, eingeräumt werden. In Abgrenzung zum Widerspruch nach § 69 VwGO sollte es „*Einwand*" genannt werden. Es bietet der betroffenen Person die Möglichkeit, gegen eine auf der Basis eines Erlaubnistatbestands an sich rechtmäßige Datenverarbeitung ihren abweichenden Willen geltend zu machen.

33. Nicht nur für öffentliche, sondern auch für nicht öffentliche Stellen, die geschäftsmäßig automatisiert Daten verarbeiten, sollte aufgrund des vergleichbaren Risikopotenzials ebenfalls eine *Gefährdungshaftung* vorgesehen werden. Um den Vollzug der Datenschutzregelungen zu unterstützen, sollte jedoch die Gefährdungshaftung entfallen und an ihre Stelle die allgemeine Haftungsregelung treten, wenn die verantwortliche Stelle nachweist, dass sie für den Zeitraum, in dem die Regelverletzung erfolgt sein kann, alle Anforderungen des Datenschutzmanagements erfüllt hat, oder am Datenschutzaudit teilnimmt. Neben materiellen Schäden sollten auch *immaterielle Schäden* anerkannt werden, wenn sie auf schweren Verletzungen des Persönlichkeitsrechts beruhen. Sie sind bei einer Verarbeitung personenbezogener Daten das eigentliche Risiko.

34. Ebenso sollte der *Kausalitätsnachweis* erleichtert werden. Wenn die betroffene Person die Rechtswidrigkeit oder Unrichtigkeit der Datenverarbeitung sowie Umstände des Einzelfalls belegt, die eine ganz überwiegende Wahrscheinlichkeit für die Ursächlichkeit des entstandenen Schaden begründen, soll die verantwortliche Stelle nachweisen müssen, dass ihr Fehler den Schaden nicht verursacht haben kann. Diese Beweismaßreduzierung trägt den Besonderheiten durch Datenverarbeitung verursachter Schäden Rechnung, bei denen eine vollständige Überzeugung des Gerichts hinsichtlich des Vorliegens der haftungsbegründenden Kausalität typischerweise nicht erreicht werden kann. Die Ursachenvermutung wird regelmäßig dann nicht eingreifen, wenn die verantwortliche Stelle nachweist, dass sie alle Anforderungen an ihr Datenschutzmanagement erfüllt hat. Der Nachweis kann auch durch die erfolgreiche Teilnahme am Datenschutzaudit erfolgen.

Effektive Datenschutzkontrolle

35. Die Datenschutzkontrolle sollte für den öffentlichen und nicht öffentlichen Bereich einschließlich der Telekommunikation, Mediendienste und Rundfunkanstalten zusammengeführt werden. Hierfür bieten sich der Bundes- und die Landesbeauftragten an. Eine solche *Vereinheitlichung* der Kontrollstellen entspricht der Europäischen Datenschutzrichtlinie und führt zu wünschenswerten Synergieeffekten. Überdies erleichtert eine Vereinheitlichung es den Betroffenen, ihre Anrufungsrechte wahrzunehmen.

36. Im Sinn einer *völligen Unabhängigkeit* der Kontrollstellen nach Art. 28 DSRL sollte die Rechtsaufsicht über die Kontrollstellen sowohl für den öffentlichen wie auch für den nicht öffentlichen Bereich neu überdacht werden. Rechtsaufsicht ist immer mit einer Einflussnahme auf die Amtsführung der beaufsichtigten Stelle verbunden. Die Einführung der Initiativkontrolle auch im nicht öffentlichen Bereich führt überdies zu einem weitergehenden Eingriff in die Privatsphäre von Unternehmen und legt eine Kontrolle über diese durch unabhängige, nicht in die Ministerialverwaltung eingebundene und von ihr kontrollierte Stellen nahe. Die notwendige demokratische Legitimation der Kontrollstellen erfolgt – wie auch heute schon – durch die Wahl der Amtsinhaber durch die Parlamente und ihre Berichtspflicht gegenüber diesen. Zur Klarstellung der Unabhängigkeit wäre eine Einrichtung des Bundesbeauftragten als oberste Bundesbehörde wünschenswert.

37. Die *Durchsetzungskompetenzen der Kontrollstellen* müssen gestärkt werden. Ihnen müssen wirksame Einwirkungsbefugnisse in die Hand gegeben werden. Bei Nichtbeachtung von Beanstandungen gegenüber öffentlichen Stellen sollte den Datenschutzbeauftragten der Verwaltungsrechtsweg eröffnet werden. Gegenüber nicht öffentlichen Stellen müssen die Kontrollstellen mit der Befugnis ausgestattet werden, die Sperrung, Löschung oder Vernichtung von Daten, die widerrechtlich verarbeitet wurden, durch Verwaltungsakt anzuordnen. Sie sollten darüber hinaus über eine umfassende Strafantragsbefugnis verfügen. Eine Erziehungsfunktion gegenüber Personen, die durch die Nichtbeachtung datenschutzrechtlicher Vorschriften eine Ordnungswidrigkeit oder Straftat begangen haben, könnte ein verpflichtender Datenschutzunterricht erfüllen, in dem Kenntnisse im Datenschutz vermittelt werden. Die in Art. 28 Abs. 2 DSRL vorgesehene Anhörung der Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, sollte als Verpflichtung der entsprechenden Stellen zur Konsultation des Bundesbeauftragten ausgestaltet werden.

38. Die Stellung der *betrieblichen und behördlichen Datenschutzbeauftragten* muss gestärkt werden. Ihre Weisungsfreiheit und Unabhängigkeit sollte durch einen verstärkten *Kündigungsschutz* unterstützt werden, der sich an dem für Mitglieder der Mitarbeitervertretung orientiert. Lediglich natürliche Personen sollten als Datenschutzbeaftragte bestellt werden können. Externe Datenschutzbeauftragte sollten nur noch für einen Mindestzeitrahmen von fünf Jahren bestellt werden dürfen, um eine Umgehung des Kündigungsschutzes zu verhindern. Die Anforderungen an *Fachkunde und Qualifikation* sowie die sachliche und personelle *Ausstattung* der Beauftragten sollten näher beschrieben werden. Das Verhältnis zwischen Datenschutzbeauftragtem und Mitarbeitervertretung muss geklärt werden. Ein neues BDSG sollte auch die Funktion eines *Konzerndatenschutzbeauftragten* aufnehmen. Dies würde zu wünschenswerten Synergieeffekten führen und die Rolle des Datenschutzes im gesamten Konzernverbund stärken. Einem vom deutschen Datenschutzrecht sanktionierten Konzerndatenschutzbeauftragten wird es darüber hinaus in weltweit tätigen Konzernen leichter fallen, Datenschutzgrundsätze im gesamten Konzern durchzusetzen.

39. Datenschutz könnte künftig auch durch eine *gesellschaftliche Kontrolle* unterstützt werden. So sollten im Rahmen des unlauteren Wettbewerbs *Konkurrentenklagen* bei Datenschutzverstößen ermöglicht werden. Ebenso sollte anerkannten Verbänden des Verbraucher- und Datenschutzes ein *Verbandsklagerecht* eröffnet werden.

Informationelle Selbstbestimmung als Grundrecht

40. Die Modernisierung des Datenschutzrechts würde unterstützt, wenn flankierend die informationelle Selbstbestimmung als *Grundrecht* der Informationsgesellschaft in das Grundgesetz aufgenommen würde. Das Grundrecht sollte nicht allein persönlichkeitsrechtlich gefasst, sondern als Kommunikationsgrundrecht ausgestaltet werden, das als Querschnittsgrundrecht den kommunikativen Gehalt aller Grundrechte zum Ausdruck bringt.

Teil 1
Zur Notwendigkeit einer Modernisierung des Datenschutzrechts

Eine Modernisierung des Datenschutzrechts ist notwendig. Sie wird einerseits motiviert aus einer *positiven Erwartung* an seine erforderliche Schutzfunktion und andererseits aus einer *zutreffenden Kritik* des gegenwärtigen Datenschutzrechts.

1. Datenschutz als notwendiger Vertrauensfaktor

Datenschutz ist Grundrechtsschutz und Funktionsbedingung eines demokratischen Gemeinwesens. Er ist notwendiger Bestandteil einer freiheitlichen Kommunikationsordnung. Teilhabe und Teilnahme an einem freien Wirtschaftsverkehr und an demokratischer Willensbildung sind nur zu erwarten, wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann. Diese ist nur möglich, wenn die Erhebung und Verwendung von Daten über ihn grundsätzlich seiner freien Selbstbestimmung unterliegt.

Datenschutz ist akzeptiert, seine Verbesserung erwünscht.[1] In einer repräsentativen Umfrage votierten 55 Prozent für einen Ausbau des Datenschutzes. Weitere 30 Prozent würden ihn zumindest auf dem Niveau von heute halten und lediglich jeder zwölfte (8%) meint, dem Datenschutz könnte gern weniger Bedeutung beigemessen werden. Am deutlichsten sprechen sich die Bewohner der neuen Bundesländer für eine Intensivierung des Datenschutzes aus. Mit zwei Dritteln stimmt eine deutliche Mehrheit für einen Ausbau des Datenschutzes. Gemeinsam mit jenen Personen, die zumindest den Grad des heutigen Schutzes beibehalten wollen, sind dies 88 Prozent.

Datenschutz ist daher auch ein Wirtschaftsfaktor. Auch wenn es sich nicht unmittelbar auf Umsatz und Gewinn umrechnen lässt, ist es etwa für Versicherungen nicht ohne Folgen, dass sie hinsichtlich eines korrekten Umgangs mit personenbezogenen Daten nur das Vertrauen von 30 Prozent der Bundesbürger genießen und damit zum Beispiel deutlich hinter dem Verfassungsschutz (41%) rangieren. Was auf den ersten Blick nur als Imagefrage erscheint, kann sich in Zukunft zur Existenzfrage ausweiten. Wenn Versicherungen nicht zugetraut wird, Datenschutz auf Dauer zu garantieren, werden sich die Verbraucher nach anderen Sicherheiten umsehen oder umorientieren. Wer mit anvertrauten Daten nicht sorgsam umgehen kann, wird in der Informationsgesellschaft des 21. Jahrhunderts einen schweren Stand haben.

Vorrangig für alle Formen des elektronischen Handels und der elektronischen Verwaltung ist Datenschutz ein entscheidender Akzeptanzfaktor. Er kann das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen vor Missbrauch von personenbezogenen Daten entgegenwirken. Erst ein wirksamer Datenschutz ermöglicht es, die hoffnungsvollen Prognosen des E-Commerce zu erreichen und eine Verwaltungsmodernisierung unter Mitwirkung der Bürger durchzuführen. Ein moderner und den neuen Technikanwendungen adäquater Datenschutz ist damit ein bedeutender Wettbewerbsfaktor und Standortvorteil.

Ein moderner Datenschutz wird darüber hinaus für alle künftigen Ausprägungen der Informationsgesellschaft und Informationswirtschaft von herausragender Bedeutung sein. Ohne ausreichenden Datenschutz werden sich viele Bürger verweigern. Er ist daher auch der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

---

[1] Alle Zahlen aus *Opaschowski*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.1.

2. Kritik am gegenwärtigen Datenschutzrecht

Der zweite Antrieb für eine Modernisierung des Datenschutzes kommt aus der berechtigten Kritik am gegenwärtigen Datenschutzrecht. Dem Datenschutzrecht ist es in der Vergangenheit zwar gelungen, den Gedanken des Datenschutzes – gegen viele Widerstände – in der Gesellschaft zu etablieren. Auch konnte es mit den Beauftragten für den Datenschutz, den Aufsichtsbehörden und den betrieblichen und behördlichen Datenschutzbeauftragte eine spezifische Vollzugsinfrastruktur aufbauen. In vielen Behörden und Unternehmen wird auf Datenschutz geachtet. Dennoch fühlen sich viele Bürger hinsichtlich der Verarbeitung ihrer Daten verunsichert und hilflos. Fast 40 Prozent der Bevölkerung in Deutschland vermuten, dass ihre Daten entgegen gesetzlichen Vorgaben bewusst missbraucht werden. Fast ebenso Viele wissen nicht, was sie dagegen tun könnten. Und weitere 13 Prozent resignieren geradezu und verweisen darauf, dass der Einzelne gar „keine Chance" der Gegenwehr habe und „da nichts machen" könne.[2] Dass jeder zweite Bundesbürger sich Datenmissbrauch ausgeliefert fühlt, korreliert mit einer vielgestaltigen Kritik, die in Fachkreisen am gegenwärtigen Datenschutzrecht geübt wird und dessen ungenügende Effizienz in vielen Bereichen beschreibt. Relevante Aspekte dieser Kritik sind:

2.1 Überholtes Konzept

Das bisherige Datenschutzkonzept sieht ein grundsätzliches Verbot vor, personenbezogene Daten zu verarbeiten. Zweckgebundene Ausnahmen bestehen nur, wenn der Betroffene einwilligt oder eine Rechtsvorschrift dies erlaubt. Das Datenschutzrecht ist vom Ansatz her orientiert an einer Datei personenbezogener Daten, die von einer verantwortlichen Stelle in einer zentralen Datenverarbeitungsanlage verarbeitet oder zu einer solchen übermittelt wird. Dieses Schutzkonzept ist in den 70er Jahren am Paradigma zentraler staatlicher Großrechner entwickelt worden, zwischen denen ein Datenaustausch die Ausnahme war. Soweit seine Konstitutionsbedingungen noch fortbestehen, vermag das bisherige Konzept den Ansprüchen zu genügen. Soweit jedoch personenbezogene Daten in weltweiten Datennetzen von vielen Beteiligten ohne durchgreifende zentrale Kontrollmöglichkeiten verarbeitet werden, muss dieses Konzept als überholt gelten und durch neue konzeptionelle Maßnahmen ergänzt oder ersetzt werden.

Die Nutzung des Internet hat dazu geführt, dass nahezu alle sozialen Handlungen auch auf dieses Medium übertragen werden. Die Abwicklung wirtschaftlicher, gesellschaftlicher, politischer und persönlicher Beziehungen über das Netz wird künftig in starkem Ausmaß zunehmen. Im Gegensatz zur Offline-Welt wird in der Online-Welt aber jede Lebensregung Datenspuren erzeugen, die in unmittelbar verarbeitbarer Form entstehen. Diese Entwicklung wird die weltweiten und regionalen, die institutionellen und privaten, die formellen und informellen Datenströme in den kommenden Jahren auf ein Vielfaches der heutigen Datenströme wachsen lassen. Dieser Entwicklung ist das Datenschutzrecht erst durch vorsichtige bereichsspezifische Regelungen gefolgt. Diese richtigen Ansätze sind weiter zu entfalten und in das allgemeine Datenschutzrecht zu integrieren. Sie werden allerdings durch den schieren Umfang der Datenverarbeitung und deren zunehmende Komplexität vor neue Herausforderungen gestellt.

Künftig ist jedoch zu erwarten, dass der Einzelne nicht nur Datenspuren seiner Handlungen in der für ihn abgegrenzten Welt des Cyberspace hinterlässt, sondern auch durch vielfältigste Handlungen in der realen Welt. Weitere Leistungssteigerungen der Informations- und Kommunikationstechnik, kleinste Sensoren und Aktoren sowie neue Materialien zur Darstellung von Daten werden dazu führen, dass tendenziell jeder Gegenstand Rechenkapazität erhält und kommunikationsfähig wird. Diese Ubiquität der Datenverarbeitung und das „Verschwinden

[2] Alle Zahlen aus *Opaschowski*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.1.

des Computers“ werden eine neue Qualität personenbezogener Datenverarbeitung bringen. Die Datenverarbeitung wird in Kleinstrechnern mit der Kapazität von Rechenzentren der 80er Jahre stattfinden. Datenverarbeitungskapazität wird in Alltagsgegenstände eingebaut sein – in der Brille, im Ohrring, in der Kaffeemaschine, in der Heizung, im Auto, im Koffer oder in jedem Verkaufsgegenstand im Kaufhaus, sogar in „intelligentem Staub“.[3] Durch kontaktlose Datenübertragung kann das Auto seinen Besitzer erkennen, die Heizung den Hausbewohner, der Ohrring den Gesprächspartner, sich auf den jeweiligen Berechtigten einstellen oder diesen an ein bestimmtes Gesprächsthema erinnern. Niemand wird mehr im Voraus wissen können, welche Daten von diesen Gegenständen erhoben und zwischen ihnen kommuniziert werden. Auf diese Entwicklung allgegenwärtiger Datenverarbeitung ist das Datenschutzrecht noch überhaupt nicht vorbereitet.[4]

Das gegenwärtige Datenschutzrecht regelt nur die geschäftsmäßige Datenverarbeitung und lässt – zu Recht – die Datenverarbeitung für rein persönliche oder familiäre Tätigkeiten außerhalb seines Anwendungsbereichs. Dieser Differenzierung wird aber zunehmend die Grundlage entzogen, wenn private und geschäftsmäßige Datenverarbeitung in der konkreten Anwendung oft nicht mehr von außen zu unterscheiden sein werden, wenn beispielsweise der mobile Mitarbeiter den gleichen Laptop, den gleichen Personal Digital Assistant, das gleiche Mobiltelefon und die gleiche Chipkarte für seine beruflichen Aufgaben und für seine persönlichen Interessen benutzt.[5] Die Probleme des Datenschutzes verlagern sich zunehmend in den Bereich des Privaten. Sie entstehen vorwiegend durch die private Nutzung von Konsum- und Unterhaltungsangeboten und manifestieren sich in der Datenverarbeitung im Rahmen medienangepasster Urheberrechts-, Marketing-, Werbe- und Abrechungskonzepte. Auch die Tatsache, dass in interaktiven Medien zwischen den Betroffenen der Datenverarbeitung einerseits und den Beteiligten an der Datenverarbeitung andererseits ein ständiger Rollenwechsel stattfindet, stellt das Datenschutzrecht vor neue, bisher unberücksichtigte Probleme. Die in der interaktiven Kommunikation anfallenden Daten können so sensible Bereiche betreffen wie die politische Einstellung, sexuelle Vorlieben, die gesundheitliche Situation oder auch religiöse Zugehörigkeiten. Durch den ständigen Rollenwechsel zwischen Vermittler und Empfänger von Informationen tragen die Mediennutzer selbst zu einer ebenso genauen wie detaillierten Kenntnis ihrer Vorstellungen, Gewohnheiten und Erwartungen aus verschiedenen Lebensbereichen bei, vor denen das Datenschutzrecht sie schützen wollte.[6]

Auch der rechtliche Rahmen für den technischen und organisatorischen Datenschutz hat sich seit Mitte der 70er Jahre kaum verändert und beruht somit noch immer auf dem Bild der Informationstechnik der damaligen Zeit. Die (geringfügigen) Fortentwicklungen der Anforderungen in den zwischenzeitlichen Novellierungsphasen änderten hieran wenig. Die von der Intention her technikfernen Regelungen des ursprünglichen Datenschutzgesetzes mit ihren abstrakten Kontrollanforderungen schienen zwar eine ständige Gesetzesanpassung entbehrlich zu machen, erwiesen sich jedoch im Lauf der Zeit gleichwohl als zu technikabhängig und gegenüber der Vernetzung, Miniaturisierung und Mobilität der Datenverarbeitung inadäquat.

Zusätzlich hat eine Verschiebung der Quantitäten und Qualitäten personenbezogener Datenverarbeitung stattgefunden: In den 70er Jahren wurde die staatliche Datenverarbeitung als Hauptbedrohung der Privatsphäre gesehen – heute gibt es bei privaten Datenverarbeitern we-

---

3 S. hierzu auch Teil 3 Kap. 8.2.2.

4 S. hierzu z.B. *Mattern*, Informatik-Spektrum 2001, 145 ff.; *Mattern/Langheinrich* 2001, 7 ff.

5 S. hierzu z.B. *Pordesch* 1995, 167.

6 S. hierzu auch *Simitis* 1997, 294; *Hoffmann-Riem*, AöR 1998, 514; *Gridl* 1999, 75; Hassemer, FR-Dokumentation, 13.7.2001, 7.

sentlich größere und sensitivere Datenbestände.[7] Viele zivilisatorische Infrastrukturleistungen werden – inzwischen – von privaten Unternehmen angeboten. Diese verfügen nicht selten über aussagekräftige Profile zu Kaufkraft, Kaufgewohnheiten und Kreditwürdigkeit. Anhand von Bewertungsmodellen wird darüber entschieden, welcher Nutzen von dem Kunden für das Unternehmen noch zu erwarten ist und auf dieser Grundlage über Kontoführung, Kredite, Energieversorgung, Telekommunikation, Versicherungen und ähnliche Dienstleistungen sowie ihre Preise entschieden. Profilhändler sind mittlerweile in der Lage, ganz spezifische Persönlichkeitsprofile zu liefern. Hierfür werden hochsensitive Daten aus der privaten Lebenssphäre erfasst, mit vielfältigen öffentlich zugänglichen Daten kombiniert und für Marketing- und andere Zwecke weiterverkauft oder zum Leasing angeboten. Besonders leicht fällt dies bei der Auswertung von Datenspuren im Internet. Das weltweit größte Unternehmen für Online-Werbung Double-Click verfügt über etwa 100 Millionen Konsumentenprofile, der zweitgrößte Anbieter Engage über 52 Millionen. Die Profile von Engage enthalten nach eigenen Angaben 800 Interessenkategorien.[8] Solche Beispiele haben auch eine Verschiebung in der Bedrohungswahrnehmung bewirkt: Der Orwell'sche „Big Brother"-Staat ängstigt die Bürger mittlerweile weniger als der unüberschaubare Datenaustausch beim modernen „Adresshandel".

Diese Beispiele zeigen auch den steigenden Wert personenbezogener Daten[9] und deren wachsende Bedeutung für die Informationswirtschaft.[10] Künftig werden Auskunftsdienste anbieten, alle gewünschten Informationen über Personen im Internet zu suchen, zu sammeln und anderen Unternehmen (Banken, Versicherungen, Arbeitgebern, Vermietern) zur Verfügung zu stellen. Weitere neue Geschäftsmodelle, die Daten oder Unterhaltung gegen die Preisgabe personenbezogener Daten anbieten (Beispiel: Yahoo!), die die freiwillige Weitergabe personenbezogener Daten gegen Gewinnbeteiligung makeln (Beispiel: Cocus),[11] die Daten unbemerkt mit Hilfe von Cookies und Web-Bugs sammeln und für personalisierte Werbung und andere Marketingzwecke verwenden (Beispiel: Double-Click, Engage)[12] oder die personenbezogene Daten für den Einzelnen treuhänderisch verwalten (Beispiel: Infomediaries)[13] spiegeln sich im bisherigen Datenschutzrecht nur ansatzweise wieder.

---

7 S. z.B. *Hassemer*, DuD 1996, 195 ff.; *ders*., Frankfurter Rundschau-Dokumentation vom 19.4.1999; *Paefgen*, CR 1994, 14 ff.; *Tauss/Kollbeck/Mönikes* 1996, 62; *Rüttgers*, CR 1996, 55; *Hoffmann-Riem* 1997, 783 ff.; *Kloepfer* 1998, D 68f.; *Schulz*, Verwaltung 1999, 140.

8 S. z. B. http://www.engage.com/uk/press/releases/2qfiscal.htm.

9 Dass es hier um Milliardenbeträge gehen kann, zeigt in eindrucksvoller Weise die Klage der Firma „Universal Image", Hersteller von Videos für Internet-Broadcasts, gegen die Firma „Yahoo!" auf insgesamt vier Milliarden US-Dollar Schadensersatz. „Yahoo!" hat nicht wie vereinbart – als Gegenleistung für die Verfügungstellung von Videos – die Registrierungs- und Nutzerdaten seines Dienstes „broadcast.com" an „Universal Image" geliefert. Die beklagte Firma wehrt sich mit dem Argument, ihre Privacy Policy erlaube die Datenherausgabe nicht – s. Heise Online, 30.12.1999, <http://www.heise.de/newsticker/data/jk-30_12_99-000.html>. S. auch den Konflikt zwischen „Alibris" und „Amazon.com" wegen des Abfangens von Kunden-E-Mails, Heise Online, 23.11.1999, <http://www.heise.de/newsticker/data/hob-23.11.99-001/>.

10 Für viele Internet-Firmen stellt die Kundendatenbank nach einer Insolvenz häufig die einzige Kapitalquelle dar. Gut gepflegte Datenbestände, die sich in die eigene Marketing-Politik einbinden lassen, sind bei der Konkurrenz sehr begehrt. S. etwa das Beispiel des Spielzeughändlers „Toysmart" der entgegen seiner Aussagen in der Privacy-Policy seine künftige Konkursmasse in Form von Kundenlisten in einer Anzeige im Wall Street Journal anbot, Heise Online, 11.07.2000, http://www.heise.de/newsticker/data/hob-11.07.00-000/.

11 Bei der Hamburger Firma „Cocus" registrieren sich die Kunden auf der Webseite <http://www.ifay.com> und geben dort detailliert Auskunft über ihre Hobbys, ihre Interessen und ihr Einkommen. Ein Data-Mining-Programm erzeugt aus diesen Datensätzen verschiedene Kundengruppen (sog. Cluster), die spezielle marketingrelevante Merkmale aufweisen. Die entsprechend aufbereiteten Datensätze werden meistbietend zum Verkauf angeboten. Der Kunde ist zu 40% am Umsatz beteiligt.

12 S. hierzu *Hillenbrand-Beck/Gress*, DuD 2001, 389.

13 S. zu diesen näher *Grimm/Roßnagel*, DuD 2000, 450 m.w.N.

Der Handel mit Daten steht erst am Anfang. Was die Werbeindustrie derzeit umtreibt, ist die Frage, wie die Form der Kundenprofile vereinheitlicht werden kann, um einen effizienten Austausch zu erreichen. Eine Reihe von Unternehmen, darunter „Macromedia", „DoubleClick", „IBM" und „Sun", wollen gemeinsam einen offenen Standard entwickeln, der es erlaubt, die mit unterschiedlichen Softwareanwendungen und Rechnersystemen von verschiedenen Geschäftspartnern gesammelten Kundendaten zusammenzuführen und gemeinsam zu nutzen. Der Standard CEPEX (Customer Profile Exchange) soll online und offline gesammelte Daten von Kunden in einer XML-basierten Datenbank integrieren, die von verschiedenen Programmen online und offline benutzt werden kann.[14]

Das Datenschutzrecht war bisher technikfern. In einem rein normativen Ansatz enthielt es fast ausschließlich Verhaltensregelungen, die sich an die verantwortliche Stelle richten und deren Einhaltung durch nachträgliche Kontrolle gewährleistet werden soll. Technische Entwicklungen und die Organisation von Datenverarbeitungsprozessen haben diese rein normativen Vorgaben immer wieder unterlaufen und dem Recht ihnen angepasste Regelungen und Konkretisierungen aufgezwungen. Beispiele sind die Einebnung rechtlich differenzierter Verarbeitungsberechtigungen durch Informationsverbünde, die unvermeidbare Verarbeitung von Überschussinformationen durch breite Erfassungsmöglichkeiten (Video, Audio, Suchmaschinen), die Datenweitergabe aufgrund von Outsourcing oder die Unmöglichkeit ein einmal im Internet verbreitetes Datum wieder zu löschen. Erst jüngste Datenschutzgesetze haben die Erkenntnis aufgenommen, dass die Gewährleistung von Datenschutz Anforderungen an Datenverarbeitungssysteme erfordert. Diese noch vorsichtigen Ansätze sind zu entfalten und in ein modernes Datenschutzrecht systematisch zu integrieren.

Die in Anlage zu § 9 Satz 1 BDSG normierten Maßnahmen spiegeln nur sehr oberflächlich die Anforderungen an die Informationstechnik und deren Möglichkeiten im Rahmen eines modernen Datenschutzes wider. So fehlt es schon im einleitenden Teil der Anlage an der Klarstellung, dass es sich bei den folgenden Anforderungen nicht nur um solche an die „Organisation" handelt. Bereits hier müsste betont werden, dass die Anforderungen sich auch und vor allem an die Gestaltung der *Technik* richten, die sowohl vom Hersteller als auch vom einzelnen Verarbeiter bei Auswahl, Einsatz und Konfiguration beachtet werden müssen.

Weder Gesetz noch Anlage definieren eine sinnvolle Sammlung von Schutzzielen der Informationstechnik, ja Schutzziele der Informationstechnik werden kaum erwähnt. Die in § 3a BDSG definierten Schutzziele „Datenvermeidung" und „Datensparsamkeit" sind zwar sinnvolle Schutzziele, es fehlt aber jede Einordnung in einen Gesamtzusammenhang zu anderen Schutzzielen wie auch zu den in der Anlage zu § 9 Satz 1 BDSG genannten Maßnahmen.

Die Anlage fordert acht Maßnahmen der Informationstechnik und Organisation zum Datenschutz. Weder wird ein Zusammenhang dieser Maßnahmen dargelegt, noch warum sie widerspruchsfrei sein sollen. Für eventuell vorhandene Konflikte ist keine Priorisierung vorgesehen. Teilweise fordert die Anlage Unmögliches und entwertet damit ihre eigene Ernsthaftigkeit: Wenn unter Nr. 4 für die Weitergabekontrolle gefordert wird, „dass ... Daten bei der elektronischen Übertragung ... nicht unbefugt ... verändert oder entfernt werden können", so kann dies in der implizierten Schärfe in Netzen mit einer größeren regionalen Ausdehnung überhaupt nicht gewährleistet werden. Informationstechnik und Organisation kann hier allenfalls gewährleisten, dass Veränderung oder Entfernung vom Empfänger mit sehr großer Wahrscheinlichkeit erkannt werden.

Erst jüngste Datenschutzgesetze haben die Erkenntnis aufgenommen, dass die Gewährleistung von Datenschutz Anforderungen an Datenverarbeitungssysteme erfordert. Diese noch

[14] S. *Möller*, DANA 3/2000, 18; *Weichert* 2000, 169.

vorsichtigen Ansätze sind zu entfalten und in ein modernes Datenschutzrecht systematisch zu integrieren.

Schließlich setzen die Globalisierung der Datenverarbeitung und die weltweite Vernetzung dem nationalen Datenschutzrecht Grenzen. Durch sie werden Daten und Datenverarbeitungsmöglichkeiten für jeden weltweit verfügbar. In Sekundenschnelle können ganze Datensammlungen über den Globus transferiert oder abgerufen werden. Im Internet gibt es keine Grenzkontrollen. Die Datenverarbeitung findet nicht in einer Datenverarbeitungsanlage statt, sondern im Netz mit einer Vielzahl von Beteiligten. Wer wo welche personenbezogenen Daten verarbeitet oder verarbeiten lässt, ist von einem Nationalstaat nicht mehr zu kontrollieren. Zwar findet das Datenschutzrecht der Bundesrepublik Deutschland immer dann Anwendung, wenn der Datenverarbeiter seinen Sitz in Deutschland hat. Gegenüber Datenverarbeitern, die über das Internet vom Ausland aus agieren, ist das deutsche Datenschutzrecht jedoch bisher machtlos.[15]

2.2 Fehlende Risiko- und Zieladäquanz

Noch immer bestehen zwar die Risiken für die informationelle Selbstbestimmung, die das Bundesverfassungsgericht im Volkszählungsurteil beschrieben hat:

> Sie ist „vor allem deshalb gefährdet, weil bei Entscheidungsprozessen ... mit Hilfe automatischer Datenverarbeitung Einzelangaben ... technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betreiber die Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.“[16]

Über diese 1983 – vor nahezu zwei Jahrzehnten – festgestellten Risiken hinaus, haben die Formen und Anwendungen der Informations- und Kommunikationstechniken aber zu einer erheblichen Verschärfung der Gefährdungen geführt:

Das Potenzial heutiger Systeme der Informationstechnik hat gegenüber dem der IT-Systeme vor 10 oder gar 20 Jahren exorbitant zugenommen.[17] Dies liegt einmal an der pro Jahrzehnt verhundertfachten Verarbeitungsleistung und Speicherfähigkeit sowie an einer flexibleren Nutzung durch den Menschen (z.B. dynamische Abfragesprachen bei Datenbanken statt sogenannte Stapelverarbeitung). Vor allem aber hat die inzwischen nahezu vollständige Vernetzung aller Rechner sowie die zunehmende Ausstattung von Rechnern mit Sensoren wie Mikrofonen und Videokameras zur Leistungssteigerung der Datenverarbeitung beigetragen.[18] Innerhalb des nächsten Jahrzehnts ist eine ähnliche Steigerung verbunden mit einer zunehmenden Mobilität von vernetzten Rechnern mit Mikrofon und Videokamera zu erwarten.[19]

Verdeckte Erhebung und Verarbeitung personenbezogener Daten geschehen mittlerweile in vielfältiger Form. Teilweise erst nach jahrelangem und weitverbreitetem Einsatz in der Praxis wurde entdeckt, dass viele Programme sogenannte „Globally Unique Identifier (GUIDs)“ in die von ihnen erstellten Dokumente abspeichern. Ein verwandtes Problem sind die verdeckten „Histories“: Hierbei werden in Dokumenten nicht nur deren letzter Zustand, sondern auch wesentliche oder gar alle Zwischenschritte ihrer Entstehung ohne Zutun der Ersteller der Dokumente abgespeichert.

---

15 *Roßnagel*, DuD 1999, 254 ff.

16 *BVerfGE* 65, 1 (42).

17 S. hierzu näher Anhang 1, S. 224.

18 S. hierzu z.B. *Pfitzmann*, DuD 2001, 194f.

19 S. hierzu näher Teil 3 Kap. 8.2.1.

Nicht mehr überschaubar wird die elektronische Datenverarbeitung, wenn viele Rechner in großen Verbünden gekoppelt sind. Durch die Möglichkeit einer Zusammenführung von für sich jeweils anonymen Daten steigt das Risiko, dass die Anonymität aufgehoben werden kann. In offenen Netzen haben Daten und Programme keinen „festen Platz“ mehr, sondern können sich weitgehend frei bewegen oder lassen sich weitgehend frei bewegen.

Die rasante technische Entwicklung führt überdies zu einer enormen Zunahme der Verarbeitung personenbezogener Daten. Allein die Kostenentwicklung von Speicherkapazitäten macht dies deutlich. War vor noch wenigen Jahren die Speicherung von Daten ein Kostenfaktor für den Verarbeiter, der zu einer zielgerichteten Speicherung führte, so ist schon heute die Speicherung nahezu kostenlos. Dies hat die Sammlung personenbezogener Daten in bisher nicht gekanntem Umfang zur Folge. Dadurch stoßen auch Anwendungen auf Interesse, die früher nicht möglich oder finanziell bei weitem nicht lukrativ gewesen wären, beispielsweise die systematische Erfassung und Auswertung aller Kundenkontakte und Kundentransaktionen, um Kundenbetreuung und Kundenlenkung zu optimieren. Durch DV-Verbünde und Werberinge findet dies im Internet sogar anbieterübergreifend, ja sogar branchenübergreifend statt.[20]

Zusätzlich gefährdet eine ungeregelte Nutzungsmöglichkeit neuer Kommunikations- und Informationstechnik die Zweckbindung der Datenverarbeitung: Große öffentliche oder quasiöffentliche Datensammlungen ermöglichen die Kombination „harmloser“ öffentlicher Daten zu Personenprofilen. Data Warehouses fassen alle in einer Organisation vorhandenen Daten in einer einheitlichen Datenbank zusammen, wo sie für jederzeitige und beliebige Auswertungen zur Verfügung stehen. Dabei gehen die Daten in der Regel losgelöst von ihrer ursprünglichen Verwendung in das Data Warehouse ein. Solche Datensammlungen sind auf Vorrat ohne Berücksichtigung einer Zweckbindung oft unterschiedlichsten Zusammenhängen entnommen. In der Praxis lässt sich meist nicht mehr feststellen, woher die Einzelinformationen im Data Warehouse stammen. Diese Datensammlungen sind auch nicht aufgrund einer Einwilligung der betroffenen Personen erstellt, zumal die Zwecke der Speicherungen und Abfragen nicht im Vorfeld beschränkt werden sollen, um dem Datenverarbeiter vielfältige Auswertungsmöglichkeiten offen zu halten. Aufgrund dieser Umstände laufen dann auch Berichtigungs- und Löschungsansprüche der betroffenen Personen leer. Für die Auswertung der Datenbankinformationen kommen Data-Mining-Werkzeuge zum Einsatz, die die automatisierte Suche nach bisher nicht bekannten Zusammenhängen in großen Datenbeständen wie Data Warehouses ermöglichen.

Scoring-Verfahren liefern aufgrund der Integration statistischer Angaben von Erfahrungen aus der Vergangenheit bestimmte Werte, die Eigenschaften einer Person, wie beispielsweise deren Kreditwürdigkeit, charakterisieren sollen. Es handelt sich dabei nicht um exakte Werte. Vielmehr geben diese Werte nur Auskunft über bestimmte statistische Wahrscheinlichkeiten. Meist wird den Betroffenen nicht mitgeteilt, welche Informationen auf welche Weise in ihren Scoring-Wert einfließen. Auch Auskunft über den Wert selbst wird oft nicht erteilt. Obwohl klar ist, dass Scoring-Verfahren nur unsichere Informationen liefern und bei ihrer Interpretation Betroffene diskriminieren können, werden sie in der Wirtschaft genutzt.[21]

Auch die Verarbeitungsformen entwickeln sich stetig fort und bringen immer neue Gefährdungen für den Schutz der informationellen Selbstbestimmung mit sich. Die Mobilität der Datenverarbeitung birgt neben dem Vorteil einer persönlicheren Verfügbarkeit personenbezogener Daten auch Risiken, da beispielsweise neue Datenkategorien anfallen: Die Kommunikationsdaten, wer, wann, von welchem Ort, wohin, mit wem kommuniziert, erlaubt beispielsweise die Frage zu beantworten: Wer befindet sich zu welcher Zeit an welchem Ort?

---

[20] S. z.B. *Hillenbrand-Beck/Gress*, DuD 2001, 389.

[21] S. z.B. *Koch*, MMR 1998, 458; *Petri*, DuD 2001, 290.

Die Erschließung neuer Medienformate, die weitere Sinne des Menschen ansprechen und teilweise simulieren, und ihre zunehmende Kostengünstigkeit ermöglichen der Datenverarbeitung, in alle Lebensbereiche vorzudringen und darüber hinaus neue Arten personenbezogener Daten (insbesondere audiovisuelle) zu erfassen.

Biometrie soll ermöglichen, dass Maschinen Menschen sicher identifizieren – genauer gesagt: wiedererkennen. Dies gelingt bisher einerseits nicht zufrieden stellend sicher, das heißt, Menschen werden nicht wiedererkannt oder sie können sich doch erfolgreich als jemand anderes ausgeben. Andererseits ermöglichen biometrische Daten und insbesondere ihre laufende Veränderung weitgehende Rückschlüsse über Krankheiten, physische und teilweise sogar psychische Vorgänge, Medikamenten-, Alkohol- und Drogenkonsum. Zudem können biometrische Referenzdaten (beispielsweise die Fingerabdrücke eines Menschen) nicht einfach durch neue ersetzt werden, sollte ihr Schutz im IT-System nicht gelingen. Dies ist anders als beispielsweise bei kryptographischen Schlüsseln, die notfalls neu verteilt werden können. Das Austeilen neuer Körper(teile), um neue biometrische Referenzmerkmale zu erhalten, ist nicht möglich.

Ubiquitous Computing wird die Aspekte der drei vorher genannten Verarbeitungsformen kombinieren: Rechner werden in alle möglichen Gegenstände unserer Umgebung eingebaut[22] – manche sagen sogar: in uns selbst. Diese Rechner kommunizieren miteinander und mit uns, indem sie biometrische Merkmale abgreifen, passend (oder auch unpassend) reagieren, vielleicht sogar manche körperlichen Vorgänge steuern können. Dies, was heutzutage noch nach Science Fiction klingt, wird in Forschungslabors weltweit zumindest in kleinem Maßstab erprobt und könnte innerhalb von zwei Jahrzehnten massenhafte Verbreitung finden. Die Auswirkungen auf den Datenschutz sind evident.

Zusammenfassend kann festgehalten werden: Dem herkömmlichen Datenschutzrecht fehlt die notwendige Risiko- und Zieladäquanz. Die ständig fortschreitende technische Entwicklung in der Datenverarbeitung wird nicht ausreichend berücksichtigt.

2.3 Intransparenz der Technik

Heutzutage wird ein Großteil der Informations- und Kommunikationstechnik im Ausland entworfen und produziert. Ihre genaue Funktionsweise inklusive aller „Nebenwirkungen“ ist dadurch in der Bundesrepublik Deutschland häufig unbekannt. Oftmals werden Geschäftsgeheimnisse und kommerzielle Interessen als angeblich gute Gründe für die Geheimhaltung der „Innereien“ von Hard- und Software angeführt. Gesetzliche Vorgaben, die diesen – nicht nur aus Sicht des Datenschutzes, sondern auch aus Sicht der nationalen, ja sogar europäischen Autonomie – höchst bedenklichen Zustand beenden, fehlen bisher.

Hinzu kommt die zunehmende Intransparenz der Datenverarbeitung. Überall werden Datenspuren erzeugt, gesammelt, ausgewertet und vermarktet. Auch die verantwortliche Stelle weiß oft selbst nicht, wo sie welche Daten verarbeitet. Die teilweise erst nach langer Zeit entdeckte Abspeicherung von „Globally Unique Identifier (GUIDs)“ in Dokumenten[23] ist ein Beispiel für ungenügende Transparenz. Vor allem in Produkten der Firma Microsoft wird mit solchen GUIDs gearbeitet. Dies blieb deshalb so lange unentdeckt, weil weder die Quelltexte der Programme öffentlich waren, so dass sie von Interessierten zur Kenntnis genommen werden konnten, noch die Datenformate. So ist etwa das Datenformat von Microsoft Word Dokumenten nicht öffentlich dokumentiert, gleichwohl sind in diesem auch GUIDs gefunden worden. Damit tragen solche Dokumente intern ein Personenkennzeichen ihres Erstellers – ohne dessen Wissen – mit sich. Auch bei automatisch erstellten „Histories“ von Dokumenten ist es

[22] S. Teil 1 Kap. 2.1.

[23] S. Teil 1 Kap. 2.2.

dem solche Dokumente Weitergebenden oftmals nicht bewusst, dass der Empfänger die genaue Entstehungsgeschichte, die auch Interna und Konflikte offen legt, zur Kenntnis nehmen kann. Der Ersatz des Übermittelns eines Papierausdrucks durch das Versenden des elektronischen Dokuments ändert also Wesentliches: Nicht nur können – sofern keine Sicherheitsmaßnahmen wie digitale Signaturen ergriffen werden – digitale Dokumente viel leichter manipuliert werden und – sofern keine wirksame Verschlüsselung erfolgt – viel leichter kopiert und weiterverbreitet werden. Elektronische Dokumente enthalten heutzutage auch Informationen, von denen der Absender nichts weiß. Dies verletzt die Anforderung nach Transparenz und Durchschaubarkeit der Datenverarbeitung grob.

Die Körperlosigkeit von Informationen verhindert eine sinnliche Wahrnehmung der Datenverarbeitungsvorgänge. Im Internet laufen zum Beispiel die von den Anbietern eingesetzten Marketingsysteme unbemerkt im Hintergrund ab.[24] Werbebanner erscheinen dem Nutzer als integraler Bestandteil der angewählten Web-Seite und nicht als Produkt eines Werbe-Netzwerks. Cookies werden regelmäßig ohne sein Wissen gesetzt und versendet. „Clickstreams" werden unbemerkt aufgezeichnet und ausgewertet.[25] Bei vielen betroffenen Personen ist die Existenz solcher Methoden und Techniken der Datensammlung noch nicht einmal bekannt.[26] Die Anbieter ihrerseits verschweigen den Einsatz und verzichten weitgehend auf Aufklärung ihrer Kunden.

2.4 Intransparenz und Widersprüchlichkeit des Datenschutzrechts

Für die unfreiwillige Erhebung und Verarbeitung personenbezogener Daten fordert das Bundesverfassungsgericht, „dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt".[27] Mit dieser Forderung wollte das Bundesverfassungsgericht Datenschutz dadurch gewährleisten, dass der Gesetzgeber eine vorbeugende Kontrolle der Datenverarbeitung sicherstellen und diese auf das erforderliche Maß begrenzen sollte.

Die ungewollte Folge dieser Forderung war jedoch eine Normenflut immer feiner differenzierender Normen für nahezu jeden Spezialbereich,[28] die das inhaltliche Ziel, die Verarbeitung personenbezogener Daten auf die wirklich unabdingbaren Fälle einzuschränken, weitgehend verfehlt hat.[29] Das Programm des Volkszählungsurteils wurde in einer Weise „erfüllt", die geradezu das Gegenteil von dem hervorbrachte, was beabsichtigt war. Statt normenklarer auch für den Bürger verständlicher Gesetze, entstand „eine häufig überdetaillierte, unübersichtliche und schwer zu vollziehende Normenmasse".[30] Die unmittelbare Bedeutung des BDSG hat dementsprechend ständig abgenommen.[31]

Der Gesetzgeber hat im öffentlichen Bereich dem Drängen der interessierten Fachbereiche kaum etwas entgegengesetzt und dem politischen Druck der jeweiligen Verarbeitungswünsche nicht zu widerstehen vermocht – wenn er dies überhaupt wollte. Im Ergebnis ist eine unübersehbare Fülle bereichsspezifischer Regelungen entstanden, in denen der Gesetzgeber

---

24 S. *Wang*, CACM 1998, 65f.

25 S. *Federal Trade Commission* 2000b, 10ff.; *Möller*, DANA 3/2000, 16f.

26 Eine Umfrage in den USA hat ergeben, dass nur 40% der Computer-Nutzer jemals von Cookies gehört haben. Business Week online, March 2000, http://www.businessweek.com/2000/00_12/b3673010.htm.

27 *BVerfGE* 65, 1 (46).

28 S. zu den Aktivitäten des Gesetzgebers in den letzten Jahren die Überblicksaufsätze zur Entwicklung des Datenschutzrechts von *Gola*, NJW 1997, 3411; NJW 1998, 3750; NJW 1999, 3753; NJW 2000, 3749.

29 S. hierzu z.B. *Bäumler* 1998, 2; *ders.*, DuD 1998, 312 ff.; *Hoffmann-Riem*, AöR 1998, 517; *Vogt/Tauss* 1998, Nr. 7; *Kloepfer* 1998, 72 ff.; *Kutscha*, ZRP 1999, 156 ff.; *Bull*, RDV 1999, 153; *Petersen* 2000, 76 ff.

30 *Kloepfer* 1998, D 72 ff.

31 *Bull*, RDV 1999, 153, stellt fest, dass es kaum noch Fälle gibt, die allein mit Hilfe des BDSG zu lösen sind; s. auch *Weichert*, DuD 1997, 712 ff.

weitgehend die jeweiligen Verarbeitungswünsche ratifiziert hat.[32] Die Funktion des Datenschutzrechts besteht damit weitgehend darin, die Voraussetzungen und Bedingungen festzulegen, unter denen personenbezogene Daten auch ohne Mitwirkung der betroffenen Person erhoben, verarbeitet oder genutzt werden dürfen.

Im nicht öffentlichen Bereich hat es der Gesetzgeber bei überaus weiten und dehnbaren Generalklauseln belassen, die ebenfalls kaum zu einer Einschränkung von Nutzungsinteressen führen. Die Interessen der Betroffenen werden im Wesentlichen offenen Abwägungsklauseln ohne präzise Abwägungsmaßstäbe überlassen. In der Regel ersetzt die mehr oder weniger freiwillige Zustimmung zu Allgemeinen Geschäftsbedingungen die Einwilligung und schafft die Absicherung für eine privat und einseitig gesetzte Verarbeitungsordnung. Zugleich fehlen in anderen Bereichen – wie Arbeitnehmer- und Kundendatenschutz – notwendige Regelungen.

Die Entwicklung des Datenschutzrechts in den letzten 20 Jahren hat dazu geführt, dass es insgesamt *überreguliert, zersplittert und unübersichtlich* ist. Niemand weiß genau, wie viele bereichsspezifische Datenschutzgesetze es im Bund und in den Ländern gibt. Der BDSG-Kommentar von *Bergmann/Möhrle/Herb*[33] nennt in einer unvollständigen Aufzählung allein etwa 110 Bundesgesetze und Verordnungen mit datenschutzrechtlichen Regelungen. Eine Juris-Recherche ergab, dass es im Bund 409 Normen (Gesetze und Verordnungen) gibt, in denen der Begriff „Datenschutz", und 401, in denen der Begriff personenbezogene Daten vorkommt. In Schleswig-Holstein beispielsweise kommt der Begriff „Datenschutz" in 183 Normen vor. Man greift sicher nicht zu hoch, wenn man von mehr als 1.000 Bundes- und Landesgesetze und -verordnungen mit Datenschutzregelungen ausgeht.

Auch das BDSG selbst ist durch die erste Stufe der Novellierung nicht einfacher und übersichtlicher geworden. Statt bisher 10.393 Wörter enthält es nun mit 15.087 Wörtern etwa um die Hälfte zusätzlichen Text.

Viele bereichsspezifische Regelungen sind schlicht überflüssig. Sie enthalten nichts anderes als die Wiederholung – bisweilen in leichter fachspezifischer Färbung – der Erhebungs-, Verarbeitungs- und Nutzungsregelungen der allgemeinen Datenschutzgesetze. So werden zum Beispiel in § 27c Abs. 3 LuftVG Allgemeinplätze des BDSG fast wörtlich wiederholt:

> „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist zulässig, soweit dies zur Erfüllung der in den Absätzen 1 und 2 genannten Aufgaben jeweils erforderlich ist. Die Daten sind zu löschen, sobald und soweit sie zur Erfüllung der Aufgaben nicht mehr benötigt werden."[34]

Ebenso wird das „Verbot mit Erlaubnisvorbehalt" des § 4 Abs. 1 BDSG wörtlich in § 3 Abs. 1 TDDSG § 3 Abs. 1 TDSV und § 1 Abs. 2 MRRG wiederholt. Die Regelungen zur Datenerhebung in § 13 Abs. 1 und 2 BDSG finden sich mehr oder minder wörtlich beispielsweise in § 179 Abs. 1 StVollzG, § 56 Abs. 4 Satz 1 BRRG, § 90 Abs. 4 Satz 1 BBG, § 36 Abs. 2 Satz 1 ZivildienstG, § 29 Abs. 2 Satz 1 SoldatenG, § 9e SeeAufgG, § 75 AuslG, § 7 AsylVfG und § 22 BKAG. Ebenso werden die Regelungen zur Datenverarbeitung und -nutzung in § 14 Abs. 1 BDSG fast gleichlautend zum Beispiel in § 180 Abs. 1 Satz 1 StVollzG, § 9e SeeAufgG, § 22 Abs. 1 PassG und § 2b Abs. 1 PersAuswG wiederholt. Die Regelungen zur Übermittlung in § 15 Abs. 1 bis 3 BDSG wurden auch nahezu gleich beispielsweise in § 10 Abs. 1 Satz 1 AZRG, § 30 Abs. 6 StVG, § 22 Abs. 1 PassG und § 25 BKAG aufgenommen. Das Auskunfts-

---

[32] S. hierzu z.B. *Bäumler* 1998, 2; *Bull*, RDV 1999, 150; *Petersen* 2000, 76f.

[33] *Bergmann/Mörle/Herb*, Systematik, Ziff. 4.2.

[34] Beispiel nach *Bull*, RDV 1999, 148. *Bull* 1998, 31f. nennt zwei weitere Beispiele: § 67e SGB X und § 288a AFG. Die Frage- und Übermittlungsbefugnis hätte wohl auch aus allgemeineren Erlaubnisbestimmungen der betreffenden Gesetze hergeleitet werden können.

recht wird beispielsweise in § 34 AZRG und § 8 Abs. 1 MRRG, das Recht auf Berichtigung in § 35 AZRG, § 489 Abs. 1 StPO, § 32 BKAG, § 8 Abs. 1 BVerfSchG und § 21 Abs. 1 BGrenzSchG, das Recht auf Sperrung in § 37 AZRG, § 32 BKAG, § 8 Abs. 1 BVerfSchG und § 21 Abs. 1 BGrenzSchG und das Recht auf Löschung in § 36 Abs. 1 Satz 3 AZRG, § 10 Abs. 1 MRRG, § 489 Abs. 2 StPO, § 32 BKAG, § 8 Abs. 1 BVerfSchG und § 21 Abs. 1 BGrenzSchG wiederholt. Ähnliches gilt etwa für die Regelungen im Sozialgesetzbuch oder in Landesschul- und Hochschulgesetzen.

Viele bereichsspezifische Regelungen regeln Selbstverständliches, das bei Anwendung allgemeiner Regelungen auch nicht anders sein könnte. Als ein Beispiel für diese Art von Datenschutzregelungen sei § 3 des Berliner Gesetzes über Datenverarbeitung im Bereich der Kulturverwaltung vom 26. Januar 1993[35] zitiert:

> §3 Eintrittskartenvertrieb von Bühnen und Veranstaltungsstätten
>
> (1) Personenbezogene Daten dürfen zum Zwecke der Reservierung und des Verkaufs von Eintrittskarten aufgrund persönlicher, telefonischer, schriftlicher, elektronischer und sonstiger Anfragen verarbeitet werden, soweit dies zur Bearbeitung der Vertriebsaufgabe erforderlich ist. Hierzu gehören insbesondere die Daten von Abonnenten kultureller Veranstaltungen, Käufern von Anrechtsscheinen, auswärtigen Klein- und Großbestellern sowie von Firmen und Vertriebsorganisationen in bezug auf Namen, Vornamen, Geburtsdaten, Anschriften, Telefonnummern, Kundennummern und sonstige Identifikationsnummern, Ermäßigungen sowie die sie begründenden Sachverhalte, Kontonummern, Zahlungsweisen, Zahlungswege, Zahlbeträge, Kontroll- und Statistikmerkmale.
>
> (2) Personenbezogene Daten werden nach Abwicklung des Vertriebsvorganges gelöscht.
>
> (3) Zum Zweck der Ermöglichung von Dienstleistungen wie Rechnungsstellung und Bilanzierung des Vertriebsgeschehens für die Kulturinstitutionen durch private Rechenzentren können personenbezogene Daten dem privaten Rechenzentrum zur Verarbeitung im Auftrag übergeben werden. Nach Abschluß der Datenverarbeitung im Auftrag sind die personenbezogenen Daten im privaten Rechenzentrum zu löschen.

Das geltende Datenschutzrecht versucht, vielen unterschiedlichen Verarbeitungskonstellationen durch immer feiner differenzierende Normen für nahezu jeden Spezialbereich gerecht zu werden, wird dadurch aber im Detail *überkompliziert* und nicht nur für den Laien, sondern auch für den Fachmann *unverständlich*.[36] Das unübersichtliche Paragraphenwerk führt leicht zu der Ansicht, Datenschutz erschöpfe sich im Wesentlichen in Formalismus und Gesetzgebungsfetischismus.[37]

Kaum nachvollziehbar ist zum Beispiel die Verwendung zweier unterschiedlicher Begriffe der Datenverarbeitung im neuen BDSG.[38] In § 3 Abs. 4 BDSG wird *Verarbeitung* in einem engen Sinn abschließend definiert als Speichern, Verändern, Übermitteln, Sperren und Löschen – ohne Erhebung und Nutzung. In § 3 Abs. 2 Satz 1 BDSG wird dagegen die *automatisierte Verarbeitung* als umfassende Verwendung personenbezogener Daten definiert, die neben dem starren Verarbeitungsbegriff des § 3 Abs. 4 BDSG auch die automatisierte Erhebung und Nutzung personenbezogener Daten enthält.

Dadurch, dass im allgemeinen Verarbeitungsbegriff Erheben und Nutzen nicht enthalten sind, müssen alle drei Verwendungsformen im Gesetz zitiert werden, wenn bei einer Regelung jeder erdenkliche Umgang mit personenbezogenen Daten erfasst werden soll. Wenn jedoch alle Formen des Datenumgangs ordnungsgemäß aufgeführt werden, wird das Gesetz nicht gerade

---

35 GVBl. 49.

36 S. z.B. *Hoffmann-Riem*, AöR 1998, 516; *Kloepfer* 1998, D 72; *Petersen* 2000, 114.

37 S. *Bäumler* 1998, 2f.; *Petersen* 2000, 84.

38 S. zum Folgenden *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 32 ff.

lesbarer oder normenklarer.[39] So werden bereits bei der Bestimmung des Geltungsbereichs in § 1 Abs. 2 Nr. 3 BDSG für den nicht öffentlichen Bereich die Begriffe Erheben, Verarbeiten und Nutzen insgesamt je vier mal zitiert:

> „Dieses Gesetz gilt für die *Erhebung, Verarbeitung und Nutzung* personenbezogener Daten durch ... nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen *verarbeiten, nutzen* oder dafür *erheben* oder die Daten in oder aus nicht-automatisierten Dateien *verarbeiten, nutzen* oder dafür *erheben*, es sei denn, die *Erhebung, Verarbeitung oder Nutzung* der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten."

Komplizierte und schwer verständliche Regelungen vermögen zwar grundsätzlich leichter dem Bedürfnis nach differenzierten Lösungen im Einzelfall gerecht zu werden, widersprechen aber der Anforderung des Bundesverfassungsgerichts,[40] dass aus dem Gesetz sich „die Voraussetzungen und der Umfang der Beschränkungen (der informationellen Selbstbestimmung) klar und für den Bürger erkennbar ergeben" müssen.[41]

Die Wiederholung von Regelungen in bereichsspezifischen Gesetzen und die Verwendung hochdifferenzierter Begriffe ist oft nur *scheinpräzise*.[42] Dies zeigt sich vor allem dann, wenn ein Begriff in einer anderen Regelung vergessen oder bewusst weggelassen wurde. Dann stellt sich nämlich die Frage, wie diese Auslassung zu bewerten ist. So soll zum Beispiel der interne Datenschutzbeauftragte nach § 4g Abs. 1 Satz 1 BDSG auf die Einhaltung des Gesetzes hinwirken, als besondere Aufgabe ist ihm durch § 4g Abs. 1 Satz 5 Nr. 1 BDSG aber nur die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme hinsichtlich der *Verarbeitung* übertragen worden. Die Überwachung der ordnungsgemäßen *Erhebung und Nutzung* fehlt jedoch. Durch die Verwendung differenzierter Verwendungsbegriffe entsteht so eine unnötige Rechtsunsicherheit.[43] Ein weiteres Beispiel bietet § 28 BDSG. Er regelt in Abs. 1 die Zulässigkeit der Datenverwendung bei nicht öffentlichen Stellen für die Phasen des Erhebens, Speicherns, Veränderns, Übermittelns und Nutzens, nicht aber für das Sperren und Löschen, obwohl diese auch Teil der Verarbeitung sind. Abs. 6 regelt für die Verwendung besonderer Arten personenbezogener Daten die Zulässigkeit für das Erheben, Verarbeiten und Nutzen – ohne wie Abs. 1 zwischen den Unterbegriffen des Verarbeitens zu differenzieren. Somit sind vom Wortlaut auch das Sperren und Löschen erfasst. Doch spricht viel dafür, dass diese in anderen Regelungen abschließend geregelt sind. Die scheinbar präzise Beschreibung des Regelungsumfangs führt somit auch in diesem Fall nicht zu einer Erleichterung der Rechtsanwendung.[44]

Scheinpräzision entsteht auch dadurch, dass trotz des Anspruchs, alles genau zu regeln, und trotz des erreichten hohen Detaillierungsgrads, auch in den bereichsspezifischen Normen nicht auf allgemeine Generalklauseln, Abwägungsregel oder Auffangnormen verzichtet wird.[45] Die Kasuistik der Spezialgesetze muss regelmäßig durch eine Auffangklausel ergänzt werden, weil die Vielfalt der in Betracht kommenden Fälle sonst nicht erfasst werden kann. Das führt zu einer Scheingenauigkeit. Statt die Verarbeitung verbindlich zu beschränken, ver-

---

39 S. *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 91; *Schild*, DuD 1997, 444f.

40 *BVerfGE* 65, 1 (44).

41 S. z.B. *Hoffmann-Riem*, AöR 1998, 516; *Petersen* 2000, 114; *Jacob*, DuD 2000, 8: „Vor dem § 28 etwa müsste selbst ein Jurist kapitulieren, der sich – unter Termindruck und vielleicht erstmals – einen raschen Überblick über die Regelungen der Datenverarbeitung für eigene Zwecke verschaffen will".

42 S. hierzu auch *Hoffmann-Riem*, AöR 1998, 516; *Bull*, RDV 1999, 148.

43 S. *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 93.

44 S. *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 94.

45 S. *Hoffmann-Riem*, AöR 1998, 516; *Bull*, RDV 1999, 148.

schwimmen ihre Grenzen immer mehr.[46] Die erhoffte Rechtssicherheit wird gerade nicht erreicht.

Die Fülle der bereichsspezifischen Regelungen führt auch zu einer Zersplitterung des Datenschutzrechts. Vielfach sind Spezialgesetze nämlich nicht mehr Konkretisierungen generell anwendbarer Grundsätze, sondern für sich bestehende und deshalb auch nur aus sich selbst heraus interpretierbare Bestimmungen.[47] Sie sind oft durch lange verschachtelte Formulierungen gekennzeichnet, nutzen mehrfache Verweise und begründen vielfältige Ausnahme- und Sonderregelungen.

Aufgrund der Normenfülle und Kompliziertheit der Regelungen bleibt es nicht aus, dass das Datenschutzrecht hinsichtlich vieler Anforderungen und Wertungen *widersprüchlich* ist.[48] Die überdifferenzierte Regelung des Datenschutzes setzt das Datenschutzrecht bei sich ständig verändernden Verarbeitungskonstellationen unter einen starken, permanenten Änderungsdruck. Die unübersichtliche Normenmasse verhindert aber konsequente und alle betroffenen Bereiche erfassende Anpassungen. Hinzu kommt, dass in unterschiedlichen Bereichen unterschiedliche Modernisierungsniveaus erreicht wurden, die auch durch die Novellierung des BDSG nur teilweise angeglichen wurden.

Wertungswidersprüche bestehen beispielsweise weiterhin im Umfang und im Verfahren der Auskunftserteilung zwischen § 7 TDDSG und § 34 BDSG, hinsichtlich der Opt-in-Regelung des § 5 Abs. 2 TDDSG und der Opt-out-Regelung des § 28 Abs. 4 BDSG hinsichtlich der Nutzung und Übermittlung von Daten für Zwecke der Werbung und der Markt- und Meinungsforschung sowie hinsichtlich der elektronischen Einwilligung nach § 3 Abs. 7 TDDSG, der Unterrichtung des Betroffenen nach § 3 Abs. 5 TDDSG und der Regelung von Profilen in § 4 Abs. 4 TDDSG, denen keine entsprechende Regelung im BDSG gegenüber steht.

Ein weiteres Problem der zersplitterten Regelungen ist die Überschneidung der Anwendungsbereiche zwischen allgemeinem und bereichsspezifischem Recht oder zwischen zwei Spezialregelungen. Ein Beispiel hierfür ist die Abgrenzung zwischen allgemeinem Datenschutzrecht, Telekommunikations- und Multimediadatenschutzrecht. Ein einheitlicher Lebenssachverhalt wird von verschiedenen Normen erfasst. Ein und dasselbe Datum fällt unter verschiedene Regelungsregime. Auf bestimmte Verarbeiter kommen verschiedene Normenkomplexe nebeneinander zur Anwendung.

Die Unübersichtlichkeit, Überkompliziertheit und Widersprüchlichkeit wirkt im Ergebnis oft vollzugshemmend und bewirkt, dass das Datenschutzrecht weniger effektiv ist, als es sein könnte und vor allem sein müsste.[49] Seine Entwicklung hat zu einer hohen Verrechtlichung der erfassten Lebensbereiche geführt. Auf viele Regelungsadressaten wirkt das Datenschutzrecht bürokratisch und ruft Abwehrreaktionen hervor, statt zu überzeugen und zu motivieren. Für den Bürger hat die Entwicklung nicht das vom Bundesverfassungsgericht beabsichtigte Ziel erreicht, ihn in die Lage zu versetzen, bereits aus normenklaren Gründen erkennen zu können, mit welcher Verarbeitung seiner Daten er zu rechnen hat. „Der Erfolg der Datenschutzidee im Recht droht zum Keim des Misserfolges von Datenschutz durch Recht zu werden."[50]

---

46 *Simitis*, DuD 2000, 715.

47 S. das Beispiel der Meldegesetze des Bundes und der Länder.

48 S. *Petersen* 2000, 79.

49 S. z.B. *Hoffmann-Riem* 1997, 782; *Petersen* 2000, 79 ff., 113.

50 *Hoffmann-Riem*, AöR 1998, 517. Zur Verrechtlichungsproblematik im Datenschutz s. auch *Donos* 1998, 186 ff.

3. Aufgaben einer Modernisierung des Datenschutzrechts

Aus der positiven Zielbestimmung und der Kritik am geltenden Datenschutzrecht lassen sich die Aufgaben einer Modernisierung des Datenschutzrechts entwickeln:

- ***Datenschutz muss effektiv werden.***

  Datenschutz darf sich nicht verzetteln. Daher muss das Datenschutzrecht sich auf die wesentlichen Bedrohungen für die informationelle Selbstbestimmung konzentrieren. Rechtliche Anforderungen müssen vollzugsgeeignet und ihre effektive Kontrolle muss sichergestellt sein.[51] Für gleichartige Bedrohungen ist ein gleichmäßiges Schutzniveau zu gewährleisten, dessen Methoden jedoch im öffentlichen und privaten Bereich unterschiedlich sein können.

- ***Datenschutz muss risikoadäquat stattfinden.***

  Es müssen Regelungen gefunden werden, die einen Schutz der informationellen Selbstbestimmung auch in einer vernetzten und in alle Lebensbereiche hineinragenden Verarbeitung personenbezogener Daten gewährleisten.

- ***Datenschutz muss verständlich werden.***

  Anforderungen und Rechte, die das Datenschutzrecht gewährt, müssen einfach, übersichtlich und klar strukturiert sein. Auf Überdifferenzierungen ist zu verzichten, auch wenn dadurch manche Ausnahme für die Datenverarbeitung oder für die Erfüllung von Pflichten entfällt.

- ***Datenschutz muss attraktiv werden.***

  Es muss für die betroffenen Personen wie auch für die Datenverarbeiter einleuchtend und sinnvoll sein, Datenschutzmaßnahmen zu ergreifen. Aufwand (Pflichten, Handhabung, Zeit, Geld) und Ertrag (Selbstbestimmung, Vertrauen, Sicherheit) müssen in einem angemessenen, besser in einem vorteilhaften Verhältnis stehen.

[51] *Zöllner*, RDV 1985, 15: Die Rechtsordnung darf nicht Verbote aussprechen, deren Nichteinhaltung einerseits gewiss und deren Sanktion andererseits nicht ernsthaft in Betracht kommt.

Teil 2
Lösungsansätze

Soweit sich Ansätze des bisherigen Datenschutzkonzepts bewährt haben, sind diese beizubehalten. Dies gilt vor allem für

- das Recht auf informationelle Selbstbestimmung als Schutzgut,
- das Datengeheimnis,
- die Meldepflichten,
- die Rechtmäßigkeitskriterien der Erforderlichkeit und der Zweckbindung,
- die Durchsetzung durch staatliche Kontrollstellen und betriebliche und behördliche Datenschutzbeauftragte,
- die Regelungen zur Datenverarbeitung im Auftrag, zu Abrufverfahren und gemeinsamen Verfahren,
- die Regelungen zu automatischen Entscheidungen,
- die Anforderungen an die Datenübermittlung ins Ausland und
- die Zweckbindung für die Kontrolldatenverarbeitung.

Diese bewährten Ansätze sind zu ergänzen, um die im Folgenden dargestellten neuen Ansätze oder Neuakzentuierungen und -konkretisierungen bewährter Ansätze. Bewährte und neue Ansätze sind in einem Gesamtkonzept zu integrieren.

1. Zielsetzungen

Die Zielsetzungen eines modernen Datenschutzrechts müssen sich an den genannten Erwartungen und an der Behebung der analysierten Defizite, soweit dies möglich ist, orientieren. Für bestimmte Herausforderungen des Datenschutzrechts – wie die Globalisierung der Datenverarbeitung und die dynamische Entwicklung der Technik – wird es keine Lösungen, sondern allenfalls verbesserte Formen im Umgang mit diesen Herausforderungen geben können.

1.1 Datenschutz durch Technik

Datenschutz muss künftig *durch*, nicht gegen Technik erreicht werden.[52] Datenschutzrecht muss versuchen, die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes auszurichten und die Diffusion und Nutzung datenschutzgerechter oder -fördernder Technik zu fördern. Datenschutz sollte so weit wie möglich in Produkte, Dienste und Verfahren integriert sein.[53]

Datenschutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung der Datenflüsse, der dynamischen Technikentwicklung und der Zunahme der Datenverarbeitung bis hin zu ihrer Allgegenwärtigkeit. Je mehr der Datenschutz dem Einflussbereich des nationalen Gesetzgebers entschwindet, desto mehr muss Datenschutz weltweit wirksam werden. Dies ist mangels einer wirksamen Weltrechtsordnung nur dann möglich, wenn er in

---

[52] S. z.B. *Podlech*, DÖV 1970, 475; *ders*, DVR 1972/73, 155; *ders*., DVR 1976, 25; *ders*. 1982, 451; *Roßnagel/Wedder/Hammer/Pordesch* 1990, 259 ff.; *Roßnagel* 1993, 241 ff.; *ders*. 2001, 13 ff.; *Simitis* 1996, 35 ff.; *Hoffmann-Riem*, AöR 1998, 537; *Vogt/Tauss* 1998, Nr. 6**;** *Bizer* 1999, 28 ff.; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 ff. Aus technischer Sicht *Pfitzmann*, DuD 1999, 405 ff.

[53] S. zum folgenden *Roßnagel*, DuD 1999, 253 ff.

die Technik eingelassen ist. Dieser Weg bietet zwei Vorteile: Datenschutztechniken sind – im Gegensatz zu Datenschutzrecht – weltweit wirksam und Technikunternehmen sind – im Gegensatz zu Gesetzgebern – sehr schnell lernende Systeme. Beide Vorteile lassen sich nutzen, wenn es gelingt, für Datenschutztechnik einen Markt zu entwickeln. Wenn sich Datenschutztechnik verkauft, wird sie sich ebenso dynamisch entwickeln wie neue technische Herausforderungen für den Datenschutz.

Technischer Datenschutz ist auch viel effektiver als rein rechtlicher Datenschutz. Was technisch verhindert wird oder unterbunden werden kann oder einfach technisch nicht möglich ist, muss nicht mehr verboten und überwacht werden. Auch wenn die Datenverarbeitung für den Einzelnen nicht mehr vorhersehbar und überschaubar ist, wirkt technisch realisierter Datenschutz auch unabhängig vom individuellen Problembewusstsein und der persönlichen Aufmerksamkeitskapazität. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen eines Techniksystems nicht. Rechtsgemäße Technikgestaltung kann Kontroll- und Überwachungsaufwand, Bußgeld- und Strafverfahren überflüssig machen.

Durch Technik müssen alle normativen Ziele unterstützt werden – nicht nur die Abschottung und Kontrollfähigkeit der Datenverarbeitung, sondern auch die Prinzipien der Transparenz, der Vermeidung des Personenbezugs, der Erforderlichkeit, der Zweckbegrenzung und Zweckbindung, der Verantwortlichkeit und der Selbstbestimmung sowie die Wahrnehmung von Betroffenenrechten. Daher ist nicht nur eine Vorschrift mit technischen Anforderungen – wie bisher in § 9 BDSG – erforderlich, vielmehr müssen technische Anforderungen in die normative Ausformung der Anforderungen an die Verarbeitung personenbezogener Daten integriert werden.

Das Datenschutzrecht darf sich nicht darauf beschränken, negative Technikfolgen zu mildern, sondern muss im Vorfeld der Entwicklung der Technik Einfluss auf deren Gestaltung nehmen. Adressaten des Datenschutzrechts können daher nicht mehr nur die für die Datenverarbeitung verantwortlichen Stellen sein. Vielmehr müssen sich die technischen Anforderungen – unter Umständen indirekt – auch an die Technikhersteller und Systemgestalter richten. Diese Anforderungen sollten von den Herstellen und Anbietern als Chance erkannt werden, unter für den deutschen Markt gleichen Wettbewerbsbedingungen weltmarktfähige Lösungen zu entwickeln, die dem Nutzer eine vertrauenswürdige Technik bieten.

1.2 Transparenz

Angesichts vielfältiger unbemerkter Datenerhebungen, der schwindenden Übersichtlichkeit der Datenströme und zunehmender Intransparenz der Technik muss es Zielsetzung modernen Datenschutzrechts sein, eine möglichst hohe Transparenz über die Verarbeitung personenbezogener Daten für die betroffenen Personen und die Kontrollstellen zu erreichen.

Wenn Selbstbestimmung über Umfang und Umstände der Selbstdarstellung und Kontrolle der Fremdzuschreibung individueller Merkmale möglich sein soll, muss die betroffene Person über ausreichende Informationen über die Erhebung personenbezogener Daten, über die Umstände und Verfahren ihrer Verarbeitung und die Zwecke ihrer Nutzung verfügen. Je undurchsichtiger und unübersichtlicher Datenverarbeitung für die betroffene Person wird, desto höhere Anforderungen sind an die verantwortlichen Stellen zu richten, der betroffenen Person die Transparenz über die von ihnen verantwortete Datenverarbeitung zu gewährleisten.

Dies setzt zum Einen voraus, dass die Informationspflichten der verantwortlichen Stelle verstärkt und die Auskunftsrechte der betroffenen Personen erweitert werden. Zum Anderen müssen aber auch alle Anwendungsabläufe, Anwendungsprogramme und informationstechnischen Abläufe (z.B. Quellcode, Compiler) – zumindest gegenüber den Kontrollstellen – offengelegt werden. Andernfalls ist eine Prüf- und Revisionsfähigkeit nicht gegeben. Wünschenswert (und für die „Fehler“suche durch die interessierte Öffentlichkeit hilfreich) ist

die weitergehende Offenlegung gegenüber allen Betroffenen und deren Interessenvertretungen.

1.3 Vermeidung des Personenbezugs

Wenn neue Erhebungs-, Speicher- und Verarbeitungskapazitäten es ermöglichen, vielfältigste Lebensäußerungen der betroffenen Personen ohne Begrenzung zu sammeln und zu unterschiedlichsten Zwecken zu nutzen, wenn die Verarbeitung personenbezogener Daten allgegenwärtig in Alltagsgegenständen erfolgt, wenn der Einzelne nicht in der Lage ist, diese vielfältigen Datenverarbeitungen zu erkennen oder zu kontrollieren, wenn viele dieser Verarbeitungen außerhalb des Einflussbereichs deutscher oder europäischer Kontrollstellen stattfinden, wenn ein einmal weitergegebenes Datum nicht mehr (sicher) wieder beseitigt werden kann – in einer Welt in der solche Bedingungen herrschen, ist Datenschutz meist nur in der Form möglich, dass der Personenbezug der Daten von Anfang an vermieden oder auf das absolut notwendige Maß begrenzt wird. Dabei geht es nicht um Sparsamkeit im Umgang mit Daten, denn Daten müssen in einer Informationsgesellschaft in breitem Umfang genutzt werden. Doch ist es oft nicht notwendig, dass diese Daten einen Personenbezug aufweisen. Die Datenverarbeitungsverfahren sind daher so zu gestalten, dass sie möglichst keinen Personenbezug und auch keine Personenbeziehbarkeit aufweisen.

Dieses Ziel kann durch Anonymität oder Pseudonymität der betroffenen Person erreicht werden. Anonymität und anonymitätsnahen Arten von Pseudonymen sollte grundsätzlich Vorrang gegeben werden. Diese auf das Erforderlichkeitsprinzip zu gründende Forderung ist als eigenständige datenschutzrechtliche Zielsetzung herauszustellen und rechtlich verbindlich zu machen.

1.4 Betroffene werden zu Teilnehmern des Datenschutzes

Das Grundrecht auf informationelle Selbstbestimmung fordert, die Autonomie der betroffenen Person anzuerkennen. Je mehr sich die Bedrohung der informationellen Selbstbestimmung in den Bereich nicht öffentlicher Datenverarbeitung verschiebt, je mehr die geschäftsmäßige und die private Datenverarbeitung zusammenwachsen und je mehr die private Nutzung von Konsum- und Unterhaltungsangeboten Datenverarbeitungsvorgänge anstößt, desto mehr muss das Datenschutzrecht die betroffene Person in die Gewährleistung ihrer Selbstbestimmung einbeziehen: Grundsätzlich muss es in ihrer Entscheidungsautonomie und -prärogative liegen, in welche Datenverarbeitungen sie einwilligt. Das Recht muss sich vielfach darauf beschränken, durch Rahmensetzungen diese Autonomie auch tatsächlich zu gewährleisten.[54]

Allerdings darf die informationelle Selbstbestimmung nicht als Herrschaftsrecht über die personenbezogenen Daten verstanden und als eigentumsähnliche Ausschluss- und Verfügungsmacht ausgestaltet werden. Ein solches Verständnis würde zum Einen den objektivrechtlichen Gehalt der informationellen Selbstbestimmung als Funktionsvoraussetzung für eine Gesellschaft verkennen, die auf individueller Selbstbestimmung und freier demokratischer Willensbildung ruht. Sie würde zum Anderen aber auch verkennen, dass personenbezogene Daten mehrrelational sind. Als Modelle der Wirklichkeit haben sie immer einen Autor und ein Objekt. Sie haben eine Beziehung zum Objekt, aber auch zum Autor. Sie können nicht allein dem Objekt zugeordnet werden.[55]

Daher kann auch die Forderung, Datenschutz dadurch zu gewährleisten, dass die betroffene Person selbst und nicht Dritte ihre personenbezogenen Daten verarbeitet, nicht in kategorischer Weise unterstützt werden. Die personenbezogenen Daten sind nicht nur Daten der be-

---

54 S. z.B. auch *Hassemer*, FR-Dokumentation vom 13.7.2001, 7.

55 In der Regel bilden die Modelle eine soziale Beziehung ab, sie betreffen dann beide Partner der Beziehung und unterliegen nicht dem alleinigen Verfügungsrecht nur einer Person - s. z.B. *Zöllner*, RDV 1985, 12.

troffenen Person, sondern ebenso der Stelle, die die Daten erhoben oder verarbeitet hat. So sind Daten über eine medizinische Behandlung zugleich auch Daten über die Leistung des Arztes, die dieser benötigt, um seinen Leistungsanspruch zu begründen und abzurechnen, um seine ärztliche Dokumentationspflicht zu erfüllen und im Streitfall eine ordnungsgemäße Behandlung nachweisen zu können. Eine Datenverarbeitung allein bei der betroffenen Person würde zum Beispiel im Verhältnis zu einer Verwaltungsbehörde gegen das Rechtsstaatsgebot, gegen die Gewährleistung gerichtlicher und parlamentarischer Kontrolle, gegen die Pflicht zur lückenlosen und wahrheitsgemäßen Aktenführung, gegen die Pflicht, konsistente und korrekte Informationen der Entscheidung zu Grunde zu legen, sowie gegen die Obliegenheiten, Beweismittel für die Rechtmäßigkeit des Verwaltungshandelns aufzubewahren und über die für die Aufgabenerfüllung erforderlichen Informationen jederzeit verfügen zu können, verstoßen.[56] Soweit dies im Einzelfall möglich ist, kann die Speicherung der Daten bei der betroffenen Person durch den Grundsatz der Erforderlichkeit geboten sein.

Grundsätzlich ist für ein mehrrelationales Wirklichkeitsmodell keine Eigentumsäquivalenz gegeben. Vielmehr ist eine Informations- und Kommunikationsordnung gefragt, die bestimmt, wer in welcher Relation befugt ist, mit dem Modell in einer bestimmten Weise umzugehen.[57] Daher wird auch nicht vom „Dateneigentümer" gesprochen, sondern von der „verantwortlichen Stelle" und der „betroffenen Person". Das Bundesverfassungsgericht hat zu Recht festgestellt, dass

> „der Einzelne ... nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten (hat); er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betreiber allein zugeordnet werden kann."[58]

Die Grundsätze dieser Informations- und Kommunikationsordnung müssen die Selbstbestimmung der betroffenen Person gewährleisten, ohne aber die rechtlich gebotene Berücksichtigung der Interessen der Autoren personenbezogener Daten zu vernachlässigen.

1.5 Datenschutz als Teil einer Informationsordnung

Im Rahmen der rechtlichen Informations- und Kommunikationsordnung deckt Datenschutz nur ein Segment ab. Es ordnet die Verarbeitung personenbezogener Daten. Die Teilhabe an Informationen,[59] eine informationelle Grundversorgung, die Verteilung von Kommunikationschancen, die kommunikative Selbstbestimmung[60] und der Schutz vor Informationen[61] – auch über einen selbst – werden von dieser Ordnung allenfalls randständig einbezogen. Diese weiteren Aspekte einer rechtlichen Informations- und Kommunikationsordnung sind für die Bürger zur Wahrnehmung ihrer Handlungsmöglichkeiten in Selbstbestimmung ebenso ent-

---

56 S. *Bizer* 2001, i.E.

57 S. hierzu auch *Simitis* 1982; *ders*. 1987, 1475, 1489 ff., insb. 1492; *Kunig*, Jura 1993, 603; *Albers* 1996, 123 ff.; *Hoffmann-Riem* 1997, 779 ff.; *ders.* 1998, 11 ff.; *ders.*, AöR 1998, 520 ff.; *Trute*, VVDStRL 57 (1998), 260 ff.; *ders*., in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5 Rn. 19; *Pitschas* 1998, M 16 ff., 29 ff.; *ders.* 1998, DuD 1998, 146 ff.; *Schulz*, Verwaltung 1999, 150; *Ladeur*, DuD 2000, 16.

58 *BVerfGE* 65, 1 (43f.).

59 S. z.B. *Kugelmann* 2001.

60 S. zu dieser für den Bereich der Telekommunikation *Roßnagel*, KJ 1990, 257 ff.; für die Mobilkommunikation *ders*. 1998, 189 ff.; für das Internet *ders*. 2000, 312f.; allgemeiner *Hoffmann-Riem* 1997, 779 ff.; *ders.* AöR 1998, 520 ff.

61 S. hierzu *Trute*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5.

scheidend wie der Datenschutz.[62] Sie bestimmen ebenso wie der Datenschutz das Informations- und Kommunikationsverhalten zwischen Bürger und Staat und der Bürger untereinander. Dieses ist daher für jeden Beteiligten nicht nur durch einen Interessenantagonismus von Datenerhebung und Datenabschottung gekennzeichnet, sondern ebenso von Informationsansprüchen und Kommunikationsbedürfnissen. Sowohl die Abwehr- als auch die Teilhabeaspekte sind Teil der Grundrechtsgewährleistung oder Voraussetzungen der Grundrechtswahrnehmung.

Auch wenn diese weiteren Aspekte einer Informations- und Kommunikationsordnung in einem Gutachten, das sich auf die Modernisierung des Datenschutzrechts konzentriert, nicht ausführlich erörtert werden können, dürfen sie nicht ignoriert werden. Ein modernes Datenschutzrecht muss als Teil einer umfassenderen Informations- und Kommunikationsordnung verstanden werden. Daher sind bei jeder Neukonzeption die Bezüge, Voraussetzungen und Auswirkungen hinsichtlich anderer Aspekte dieser Ordnung zu berücksichtigen.

Dies gilt insbesondere hinsichtlich des Rechts auf Information. „Es gehört zu den elementaren Bedürfnissen des Menschen sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten. Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie."[63] Zugang zu Informationen im öffentlichen Bereich und Datenschutz sind in einer Informationsgesellschaft keine Gegensätze, sondern zwei Seiten der informationellen Selbstbestimmung. Allerdings muss bei Auskunftsersuchen, die Unternehmensdaten oder personenbezogene Daten betreffen, ein Ausgleich zwischen dem Informationsinteresse einerseits und dem Schutz von Geschäfts- und Betriebsgeheimnissen oder der Entscheidungsprärogative der betroffenen Person andererseits gefunden werden. Dieser Zusammenhang zwischen Informationsfreiheit und informationeller Selbstbestimmung ist zu berücksichtigen,[64] jedoch sind Fragen eines Informationsfreiheitsgesetzes nicht Gegenstand des Gutachtens.

2. Konzepte der Umsetzung

Datenschutz muss in die Datenverarbeitung integriert werden. Dies kann rechtlich als Pflicht der verantwortlichen Stelle oder des Anbieters von Datenverarbeitungssystemen und/oder als Rechte der Betroffenen ausgestaltet werden. Über die als strikte normative Regelungen ausgestalteten Ansätze hinaus sind auch unterschiedliche Instrumente zu schaffen, die Anreize schaffen, System- und Selbstdatenschutz umzusetzen.

2.1 Systemdatenschutz

Den Herausforderungen durch dynamische Technikentwicklung, allgegenwärtige Datenverarbeitung, für den Einzelnen unübersichtliche Strukturen, unbemerkte Datenerhebungen und undurchschaubare Verarbeitungsformen kann vor allem durch Systemdatenschutz begegnet werden.[65] Dieses Konzept setzt die Unterstützung des Datenschutzes durch Technik um und bezieht auch den Aspekt der Organisation mit ein. Ein modernes Datenschutzrecht sollte ei-

---

62 S. hierzu *Schoch*, VVDStRL 57 (1998), 158; *Trute*, VVDStRL 57 (1998), 213 ff.; *Pitschas*, DuD 1998, 139 ff.; *ders.* 1998, M 27 ff.; *Hoffmann-Riem* 1998, 11 ff.; *Burchard*, KritV 1999, 239, 246f.; *Kugelmann* 2001; *Trute*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5.

63 *BVerfGE* 27, 71 (81f.).

64 S. z.B. die Forderung nach Anonymisierung und Pseudonymisierung personenbezogener Daten im öffentlichen Bereich, um den Informationsanspruch im Konflikt mit dem Datenschutz praktikabel zu machen – s. Teil 3 Kap. 3.4.1 – oder die Kompatibilisierung der Übermittlung von Daten von öffentlichen Stellen an nicht öffentliche Stellen – s. Teil 3 Kap. 3.5.5.

65 S. hierzu z.B. *Podlech* 1982, 451 ff.; *Roßnagel* 1994, 227 ff.; *Büllesbach/Garstka* 1997, 383 ff.; *Hoffmann-Riem* 1997, 786; *ders.*, AöR 1998, 535; *Bizer* 1999, 28 ff.; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 ff.

nen Systemdatenschutz vorsehen, der sicherstellt, dass das technisch-organisatorische System nur zu der Datenverarbeitung in der Lage ist, zu der es rechtlich auch ermächtigt ist, und die verantwortliche Stelle nur die Daten verarbeitet, die sie rechtlich verarbeiten darf. Technik und Organisation der Datenverarbeitung gewährleisten oder ermöglichen Datenschutz und verhindern Datenmissbrauch. Im Vordergrund stehen die Vermeidung des Personenbezugs und die Zweckbindung durch

- Organisation der Datenerfassung und -verarbeitung in der Form, dass personenbezogene Daten nur im unvermeidbaren Umfang erhoben und verarbeitet werden (Ein Leistungsangebot nach Zeittakt erspart, Inhalte zu speichern, und ein Leistungsangebot nach „Flatrates“ erspart, Zeittakte zu speichern),
- eine informationelle und technisch abgesicherte Gewaltenteilung, die gewährleistet, dass die verantwortliche Stelle nur die Daten verarbeitet, die sie rechtlich verarbeiten darf (Bei elektronisch bestellten, aber physisch auszuliefernden Gütern, erübrigt eine datenaufteilende Systemorganisation, dass der Verkäufer Name und Anschrift des Käufers, der Auslieferservice Ware und Preis kennen müssen),
- die Gewährleistung der Infrastrukturvoraussetzungen, um anonyme Kommunikation – etwa durch MIX-Infrastrukturen – oder pseudonyme Kommunikation – etwa durch Angebote von pseudonymen (qualifizierten) Zertifikaten (Arzt, Apotheker, Anwalt) und Kommunikationsadressen sowie sonstigen (Geld-)Garantien – zu ermöglichen,
- feingranulare Pseudonymität, das heißt, Pseudonyme werden Personen nicht über mehrere Zwecke oder gar mehrere Lebensbereiche zugeordnet, sondern für jeden Zweck wird ein anderes Pseudonym verwendet.

Entsprechende Anforderungen zielen vor allem auf die Konzeption und Rekonzeption von Datenverarbeitungsstrukturen. Regelungen zum Systemdatenschutz haben jedoch den Nachteil, dass sie nur gegenüber Stellen im Inland durchzusetzen sind. Gegenüber ausländischen Stellen kann nur das Vorbild nachahmend wirken, wenn aus datenschutzkonformen Konstruktionen ein Wettbewerbsvorteil erwächst.

2.2 Selbstdatenschutz

Statt selbst die Verantwortung für den Datenschutz auch in den Fällen zu tragen, in denen er ihn gar nicht mehr gewährleisten kann, muss der Staat den einzelnen Bürger und das einzelne Unternehmen[66] durch technische Hilfsmittel und durch Infrastrukturleistungen in die Lage versetzen, sich selbst zu schützen.

Ein modernes Datenschutzrecht benötigt daher Regelungen, die Selbstdatenschutz ermöglichen, die also der betroffenen Person eigene Instrumente in die Hand geben, ihre informationelle und kommunikative Selbstbestimmung sowie ihre Geheimnisse selbstbestimmt zu schützen.[67] Sie kann so durch eigene Maßnahmen die ihr erwünschte Verarbeitung ihrer Daten ermöglichen und unzulässige Datenverarbeitung verhindern.[68] Dieser Ansatz vermag in vielen Fällen eine adäquate Antwort auf die dynamische technische Entwicklung und die

---

[66] Datenschutz sollte nicht allein aus dem Persönlichkeitsrecht, sondern auch aus den Geheimnisse schützenden Grundrechten der Art. 5, 10, 12 und 14 begründet werden - s. hierzu auch *Kloepfer* 1998, 84 ff.

[67] S. zum Selbstdatenschutz z.B. *Borking*, DuD 1996, 654; *ders*., DuD 1998, 636; *ders.*, DuD 2001, 411; *Roßnagel*, ZRP 1997, 26; *Hoffmann-Riem* 1997, 786f.; *ders.*, AöR 1998, 532 ff.; *Schneider/Pordesch*, DuD 1998, 645; *Schrader*, DuD 1998, 128; *ders*., 1998, 206; *Cranor* 2000, 107; *Trute*, VVDStRL 57 (1998), 263f.; *Enzmann*, DuD 2000, 535.

[68] S. hierzu bereits *Roßnagel/Wedde/Hammer/Pordesch* 1990, 220; s. hierzu auch *Kloepfer* 1998, D 99f.; *Hassemer*, FR-Dokumentation vom 13.7.2001, 7, weist darauf hin, dass durch Selbstschutz auch das Verhältnis zwischen staatlicher Sicherheitsgewährleistung und Freiheitssicherung entspannt werden kann.

Globalisierung der Datenströme zu bieten. Er verspricht zwei Vorteile: Der Bürger oder das Unternehmen sind aus Eigeninteresse ebenfalls ständig lernende und sehr rasch reagierende Systeme. Daher ist es – wo dies möglich erscheint – sinnvoller, sie in die Lage zu versetzen, den ihnen jeweils wichtig erscheinenden Selbstschutz jederzeit realisieren zu können, als sie durch flächendeckende Vorgaben zwangsweise zu beglücken. Außerdem wirkt dieser Ansatz weltweit: Die Selbstschutztechniken können grundsätzlich bei allen Kontakten in globalen Netzen Anwendung finden.[69]

Angesichts netzgestützter interaktiver Medien und den damit verbundenen Rollenwechseln zwischen Datenverarbeiter und betroffener Person muss das Konzept der Datensicherheit zum Konzept der *mehrseitigen Sicherheit* weiterentwickelt werden, die jedem Teilnehmer die Möglichkeit bietet, selbst seine Interessen zu schützen und mit dem Kooperationspartner die Bedingungen gegenseitiger Sicherheit auszuhandeln.[70] Systeme der Informationstechnik werden so gestaltet, dass jeder Nutzer anderen nur minimal zu vertrauen braucht – und entsprechend die Notwendigkeit von Vertrauen zwischen den die Personen und ihre Interessen repräsentierenden Rechnern ebenfalls minimiert werden kann. Dies impliziert, dass beispielsweise nicht darauf gesetzt wird, dass erfassbare Daten nicht erfasst und verarbeitet werden, sondern dass bereits die Erfassbarkeit der Daten durch geeignete Systemgestaltung vermieden wird. Derartige Maßnahmen sind mit einigem informationstechnischen Aufwand verbunden, allerdings wegen der exorbitanten Leistungssteigerung der Informations- und Kommunikationstechnik, die mehrseitige Sicherheit gerade notwendig macht, zunehmend praktikabel und angemessen.

Mittel zum Schutz personenbezogener Daten durch die betroffene Person selbst müssen entwickelt oder angepasst werden.[71] Dieser Selbstdatenschutz kann als Recht, Anspruch oder faktische Möglichkeit des Betroffenen (die rechtlich gefördert und nicht behindert wird) ausgestaltet werden:

- selbstbestimmte Nutzung von technischen und organisatorischen Schutzinstrumenten,
- einfach zu bedienende Instrumente für:
  - Inhaltsschutz (Konzelation, Steganographie),
  - Anonymität, Pseudonymität, Identitätsmanagement,
- Transparenz und Selbstbestimmung bei jeder Kommunikation, (P3P, Opt in, Opt out).

Soweit keine Identifizierung erforderlich ist, vermag die betroffene Person sich vor unerwünschter Erhebung ihrer personenbezogenen Daten am besten durch anonymes Handeln zu schützen. Soweit aber eine Identifizierung, Wiedererkennung oder Berechtigungsprüfung erforderlich ist, kommt dem Konzept pseudonymen Handelns besondere Bedeutung zu.[72] Denn

---

[69] Im Rahmen des WWW-Konsortiums werden z.B. Bemühungen unternommen, mit der „Platform for Privacy Preferences (P3P)“ den Nutzern Möglichkeiten in die Hand zu geben, bei WWW-Abrufen selbst zu bestimmen, welche Daten über den Abruf gespeichert und weiterverwendet werden – s. http://www.w3.org/P3P; *Cavoukian u.a.*, DuD 2000, 475 ff.; *Cranor*, DuD 2000, 479; *Grimm/Roßnagel* 2000a, 293 ff.; *dies*. 2000b, 157; *Wenning/Köhntopp*, DuD 2001, 139 ff.; *Gress*, DuD 2001, 144 ff.

[70] S. hierzu näher *Müller/Pfitzmann* 1997; *Müller/Stapf* 1998; *Müller/Rannenberg* 1999; *Federrath/Pfitzmann* 1998, 166.

[71] S. hierzu z.B. *Federrath/Pfitzmann*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.2; *dies*. 2001, 252 ff.; *Köhntopp*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.3; *Cranor* 2000, 107 ff.; *Grimm/Löhndorf/Roßnagel* 2000, 133 ff.; *Bizer* 1999, 54f.

[72] S. hierzu auch *Roßnagel* 1994, 245f.; *provet/GMD* 1994, 210 ff.; BT-Drs. 13/7385, 23; *Roßnagel*, in: *ders*., RMD 1999, Einführung, Rn. 61f.; *Bizer*, in: *Roßnagel*, RMD 1999, § 3 TDDSG, Rn. 174 ff.; *Federrath/Berthold* 2000, 189.

es vermag den Zielkonflikt zwischen notwendiger Identifizierung[73] des Geschäftspartners und dem Wunsch der betroffenen Person nach Anonymität[74] aufzulösen.

Um systematisch Selbstdatenschutz zu ermöglichen, ist auch eine entsprechende Unterstützung erforderlich, die bei möglichst vielen Bürgern die soziale und technische Kompetenz hierzu herstellt.[75] Diese muss von der Förderung von Programmen, die Schlüssel, Identitäten und Pseudonyme verwalten und den Nutzer bei der Verwendung von Selbstschutztechniken unterstützen,[76] bis hin zu einer neuen Bildungsoffensive reichen. Hier können auch Datenschutzbeauftragte neue Aufgaben finden, nämlich die Technikentwicklung anzustoßen, zu begleiten und nachzuvollziehen[77] sowie für die Bürger Berater in Sachen Selbstschutz zu sein.[78]

2.3 Anreize zur Verbesserung von Datenschutz und Datensicherheit

Administrativer Datenschutz, der mit Ge- und Verboten arbeitet und diesen mit Strafandrohung Nachdruck verleiht, ist notwendig, sollte aber auf das notwendige Maß beschränkt werden, um ein Mindestniveau an Datenschutz zu gewährleisten. Um dessen Akzeptanz zu stärken und seine ständige Fortentwicklung entsprechend den sich verändernden und zunehmenden Risiken zu ermöglichen, muss ein modernes Datenschutzrecht daneben aber auch Anreize für einen effektiven und sich fortentwickelnden Schutz bieten. Beispiele sind

- vertrauenswürdige Auditierung von Datenschutzmanagementsystemen und eine rechtlich abgesicherte Möglichkeit, deren Ergebnisse im Wettbewerb zu nutzen,
- vertrauenswürdige Zertifizierung datenschutzgerechter Produkte und rechtliche Anforderung, diese bei Beschaffungen der öffentlichen Hand zu bevorzugen,
- Erleichterung der rechtlichen Anforderungen bei hoher Transparenz der Datenverarbeitung, bei erfolgreicher Teilnahme an Auditierungssystemen oder Verwendung zertifizierter datenschutzfreundlicher Produkte einschließlich geeigneter Konfiguration,
- innerorganisatorische Maßnahmen zur Generierung von Risikoinformationen und Aktivierung von Lösungskapazitäten sowie von innerorganisatorischen Mechanismen der Wahrnehmung von Datenschutzinteressen.

Angesichts einer akzelerierend fortentwickelten Technik, immer neuen Geschäftsmodellen in der Verwertung personenbezogener Daten, kaum vorhersagbaren Anwendungsfeldern der netzgestützten und der ubiquitären Datenverarbeitung genügen keine isolierten Antworten auf einzelne Sachprobleme mehr. Benötigt werden vielmehr Strukturlösungen. Erforderlich ist, lernfähige Systeme zu etablieren, die auf sich ständig ändernde Herausforderungen immer wieder neue Antworten zu geben vermögen.

---

73 S. zu Missbrauchsmöglichkeiten von Anonymität *Caronni*, DuD 1998, 623 ff.

74 Zur datenschutzrechtlichen Bedeutung von Anonymität s. z.B. *Simitis* 1997, 309; *Bizer* 2000, 59; *Holznagel/Sonntag* 2000, 72; *Hamm* 2000, 90; zu Anonymitätstechniken s. *Chaum*, Communications of the ACM 1981, 84; *ders*., Communications of the ACM 1985, 1030; *Borking*, DuD 1996, 654.; *ders*., DuD 1998, 636; *ders*, DuD 2001, 411; *Arbeitskreis Technik* der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DuD 1997, 709 ff.; *Pfitzmann* 2000, 9; *Pfitzmann/Waidner/Pfitzmann*, CR 1987, 712, 796 und 898; *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 243 und 305; *Federrath/Pfitzmann*, DuD 1998, 628 ff.; *Demuth/Rieke*, DuD 1998, 623 ff; *dies*., 2000, 38; *Roessler*, DuD 1998, 619 ff.; *Köhntopp* 2000, 43.

75 S. hierzu *Hoffmann-Riem* 1997, 786f.; *ders.*, AöR 1998, 532, 534.

76 S. BT-Drs. 13/7385, 22; s. hierzu ausführlich *Roßnagel/Haux/Herzog* 1999; *Pordesch*, DuD 1999, 81; *Köhntopp* 2000, 43.

77 S. *Fox* 1998, 81; *Federrath/Pfitzmann* 1998, 166; *Müller* 1998, 173; *Kessel* 1998, 182.

78 S. auch *Schrader* 1998, 206; *Weichert* 1998, 213.

3. Neue Grundsätze des Datenschutzrechts

In der normativen Umsetzung des Datenschutzes sollen *Übersichtlichkeit, Verständlichkeit, Problemadäquanz* und *Akzeptanz* dadurch erreicht werden, dass vor allem folgende Grundsätze beachtet werden:

3.1 Klare Struktur

Um die Normenflut einzudämmen, Rechtszersplitterung zu verringern und Widersprüche zu vermeiden, sollte die Vorrangregelung im Verhältnis zwischen BDSG und bereichsspezifischen Regelungen umgedreht werden. Notwendig ist eine klare Unterscheidung zwischen einem allgemeinen Datenschutzgesetz, das allgemein verbindliche Grundsätze für alle Datenverarbeitungsbereiche und -phasen enthält und Rechte der Betroffenen begründet, und bereichsspezifischen Regelungen, die nur noch explizite Ausnahmen von diesen Grundsätzen (insbesondere Erlaubnistatbestände) enthalten.

Das allgemeine Gesetz soll verständliche und präzise Anforderungen an die Datenverarbeitung enthalten und damit Klarheit für betroffene Personen und Datenverarbeiter über einen für beide verbindlichen Rahmen bieten. Offene Abwägungsklauseln sollen angesichts der damit verbundenen Rechtsunsicherheit vermieden werden.[79] Die rechtlichen Voraussetzungen der Datenverarbeitung müssen auf grundsätzlicher Ebene möglichst exakt beschrieben werden. Das Gesetz muss sich auf das Wesentliche konzentrieren und auf anspruchsvollem Niveau das Mögliche und Durchsetzbare beschreiben. Unvermeidbare Ausnahmen von den Grundsätzen sind ebenfalls in das allgemeine Gesetz aufzunehmen. Auf eine Subsidiaritätsklausel wird verzichtet. Das allgemeine Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten.

Spezialregelungen in bereichsspezifischen Gesetzen sollten nur Ausnahmen von den allgemeinen Regelungen enthalten.[80] Diese können für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten. Auch könnten Ausnahmen vorgesehen werden, wenn Aufgaben im Allgemeininteresse ansonsten nicht erfüllt werden können. Alle Ausnahmen sind als explizite Durchbrechungen der allgemeinen Prinzipien durch Formulierungen wie „... in Abweichung von § X BDSG...“ kenntlich zu machen. Dieses Vorgehen gibt dem jeweiligen Gesetzgeber die Begründungslast für die Unvermeidbarkeit der Abweichung und macht die Abweichung den Normadressaten unmissverständlich deutlich.

Das moderne BDSG ist nicht subsidiär. Es enthält die grundsätzlichen Regelungen des Datenschutzrechts, die „vor die Klammer gezogen werden können“.[81] Es derogiert damit alle bereichsspezifischen Regelungen. Um diese, soweit sie von den allgemeinen Grundsätzen abweichen, nicht gleichzeitig auch novellieren zu müssen, ist eine Übergangsregelung erforderlich. Nach dieser sollte die Vorrangregelung des BDSG für bereits bestehende widersprechende Gesetze erst nach vier Jahren in Kraft treten. In dieser Frist können die bereichsspezifischen Regelungen angepasst oder als explizite Ausnahmen ausgestaltet werden. In dieser Übergangszeit gilt das novellierte BDSG unmittelbar für den nicht öffentlichen Bereich sowie den nicht speziell geregelten öffentlichen Bereich. Für speziell geregelte Bereiche wirkt es als Auslegungsrichtlinie.[82]

---

79 Zur Kritik s. z.B. *Simitis*, in: *ders*. u.a., BDSG, § 28 Rn. 147; *Simitis*, JZ 1986, 190; *Bühnemann*, BB Beilage zu Heft 3/1974, 1, 5; *Mallmann*, CR 1988, 95.

80 Die beispielhaft in Teil 1 Kap. 2.4 genannten Vorschriften aus bereichsspezifischen Gesetzen und viele mehr könnten dann ersatzlos entfallen.

81 S. auch *Bull*, RDV 1999, 148, 153.

82 S. Teil 3 Kap. 10.

Das Gutachten erfasst nicht Sonderprobleme des bereichsspezifischen Datenschutzes, wie sie sich etwa im Sicherheitsbereich, im Arbeitnehmer- und Sozialdatenschutz stellen. Welche Ausnahmen und Anpassungen in diesen Bereichen notwendig sind, wird im Gutachten nicht im Detail erörtert.

3.2 Einheitliche und umfassende Regelungen

Um den neuen Gefährdungslagen der informationellen Selbstbestimmung im nicht öffentlichen Bereich gerecht zu werden sowie um die Regelungsstruktur zu vereinfachen und ihr Verständnis zu erleichtern, sollten die allgemeinen Datenschutzgrundsätze für den öffentlichen und für den nicht öffentlichen Bereich gleichermaßen gelten.[83] In beiden Bereichen ist – risiko- und nicht bereichsabhängig – das gleiche Datenschutzniveau zu gewährleisten. Unterschiede auf Grund der Grundrechtsbindung im nicht öffentlichen Bereich und der Verfolgung von Allgemeininteressen im öffentlichen Bereich können durch unvermeidbare Ausnahmeregelungen – je nach Allgemeinheitsgrad in den allgemeinen oder in bereichsspezifischen Regelungen – berücksichtigt werden.

Die Grundsätze sollten auch nicht zwischen manueller und automatischer Datenverarbeitung unterscheiden. Sie sollten sich grundsätzlich auf alle personenbezogenen Daten erstrecken, die nicht zu persönlichen oder familiären Zwecken verarbeitet werden. Soweit zweckmäßig können einzelne Pflichten auf Dateien oder die automatisierte Datenverarbeitung beschränkt werden.

3.3 Vereinheitlichung auf hohem Niveau

In Zeiten des elektronischen Geschäftsverkehrs und der elektronischen Verwaltung nimmt die Bedeutung der Telekommunikation für die Verarbeitung personenbezogener Daten erheblich zu. Für die Zukunft ist sogar zu erwarten, dass Datenverarbeitung ohne Telekommunikation die Ausnahme sein wird. Daher erscheint es nicht mehr zeitgemäß, diesen Bereich in Spezialgesetzen zu regeln. Da die Möglichkeiten der Telekommunikation die Praxis der Datenverarbeitung so stark bestimmen wird und das Datenschutzrecht der Telekommunikation und der Teledienste das fortschrittlichste Niveau aufweisen, sollte dieses zum Ausgangspunkt der Novellierung gewählt werden.

Das Telekommunikations- (§§ 85 und 89 TKG und TDSV) und Teledienstedatenschutzrecht (TDDSG) sollten daher in das BDSG integriert werden. Dadurch könnten Wertungswidersprüche und Überschneidungen der Anwendungsbereiche beseitigt und eine Vereinheitlichung auf hohem Niveau erreicht werden. Viele Regelungen dieser Regelungsbereiche – wie etwa zur Unterrichtung, zu Opt-in-Regelungen, zur Vermeidung des Personenbezugs, zur elektronischen Einwilligung oder zur Auskunft können verallgemeinert werden und sollten das allgemeine Datenschutzniveau bestimmen, andere Regelungen wie die zu Nutzungs- und Abrechnungsdaten, zum Einzelentgeltnachweis (z.B. Ticketing-Systeme, Urhebermanagementsysteme), zu Löschungspflichten oder zu technischen Sicherungen können vereinheitlicht werden.

3.4 Entlastung durch Einwilligung und Selbstregulierung

Administrativer Datenschutz muss sich auf das Wesentliche konzentrieren. Der Gesetzgeber darf keine Perfektionsansprüche verfolgen und nicht versuchen, jedes einzelne Datum, das etwa die Deutsche Oper für ihre Abonnentenverwaltung erheben darf, gesetzlich zu regeln. Da allerdings dennoch im Einzelfall bestimmt sein muss, ob ein Datum erhoben werden darf, muss der Regelungsbedarf durch andere, nämlich die Parteien der Verarbeitungsbeziehung,

---

[83] S. die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.3.1996 und vom 23./24.10.1997 sowie die Stellunganhme der Konferenz zum Gutachtendesign, das diesem Gutachten voranging (s. Anlage); s. z.B. auch *Hoffmann-Riem* 1998, 17; *Vogt/Tauss* 1998, Nr. 8.

befriedigt werden. Eine Eindämmung der Normenflut, eine Vereinfachung des Datenschutzrechts und eine Entlastung des Gesetzgebers kann nur dann erfolgen, wenn der Gesetzgeber sich auf Grundsätze der Datenverarbeitung beschränkt und deren Ausfüllung weitgehend der Selbstbestimmung der betroffenen Person oder der Selbstregulierung der Datenverarbeiter überlässt.

Im Einzelfall muss die Datenverarbeitung grundsätzlich durch Einwilligung oder Einwilligungssurrogate wie Vertrag und vertragsähnliches Vertrauensverhältnis oder Antrag gegenüber einer Behörde erlaubt werden können.[84] Da aber zwischen den betroffenen Personen und den verantwortlichen Stellen in der Regel ein erhebliches Machtgefälle besteht, muss die Selbstbestimmung gestärkt werden. Ziel eines modernen Datenschutzrechts muss es daher sein, einerseits die Zulässigkeit der Datenverarbeitung im vertretbaren Umfang der individuellen Selbstbestimmung zu überlassen, andererseits aber deren Freiwilligkeit durch Rahmenregelungen abzusichern[85] und schließlich die Mitwirkung der betroffenen Personen durch praktikable Datenschutzrechte zu ermöglichen.[86]

Allgemeine Konkretisierungen der gesetzlichen Grundsätze können durch branchenspezifische Selbstregulierung erfolgen. Um in dieser ein faires Verfahren, einen angemessenen Interessenausgleich, die Berücksichtigung von Gemeinwohlinteressen und eine gewisse demokratische Legitimation zu gewährleisten, muss der Gesetzgeber auch für diese Regelsetzung einen gesetzlichen Rahmen vorgeben.[87]

3.5 Kooperation und Wettbewerb

Das Datenschutzrecht sollte die Zusammenarbeit mit den Regelungsadressaten suchen. Wo die Datenverarbeiter durch eigene Aktivitäten einen ausreichenden Datenschutz erreichen, sollte sich der Staat zurückziehen. Zur Sicherung seiner Gewährleistungsverantwortung sollte er aber für Selbstregulierung und Selbstkontrolle einen rechtlichen Rahmen setzen, der die Zielerreichung sicherstellt und bei deren Versagen Ersatzmaßnahmen vorsieht. In das allgemeine Datenschutzkonzept sind daher als integrierte Bausteine aufzunehmen:

- Möglichkeiten der regulierten Selbstregulierung,
- Selbstkontrolle als primäre Kontrollform,
- freiwillige, rechtlich abgesicherte Auditierungs- und Zertifizierungssysteme.

4. Verfassungsrechtliche Zulässigkeit der Neukonzeption

Die Verfassungsordnung gewährt dem Gesetzgeber einen weiten Prognose- und Gestaltungsspielraum,[88] den er durch politische Prioritätensetzung füllen kann. Dennoch wirft die Neukonzeption des Datenschutzrechts vor allem in zweierlei Hinsicht verfassungsrechtliche Fragen auf: Diese betreffen zum Einen die grundsätzliche Gleichbehandlung der Datenverarbeitung im öffentlichen und nicht öffentlichen Bereich und zum Anderen die Umkehrung des Verhältnisses von allgemeinem BDSG zu den bereichsspezifischen Datenschutzregelungen mit dem Ziel, diese weitgehend zu reduzieren. Um beide Fragen beantworten zu können, soll von der Rechtsprechung des Bundesverfassungsgerichts ausgehend untersucht werden, welche verfassungsrechtlichen Verpflichtungen und Begrenzungen der Gesetzgeber für eine Neukonzeption des Datenschutzrechts zu beachten hat. Zwischen den verfassungsrechtlichen

---

84 S. Teil 3 Kap. 3.1.

85 S. näher Teil 3 Kap. 3.2.

86 S. näher Teil 3 Kap. 7.

87 S. näher Teil 3 Kap. 6.

88 S. z.B. *Schulz*, Verwaltung 1999, 148.

Markierungen einer Gesetzgebungspflicht und einer Gesetzgebungsgrenze liegt der Bereich politischer Schwerpunktbildungen und gesetzgeberischer Gestaltungsspielräume.

4.1 Schutz der informationellen Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung ist die verfassungsrechtliche Antwort auf die besonderen Risiken der automatischen Datenverarbeitung für die Selbstbestimmung des Einzelnen. Diese sieht das Bundesverfassungsgericht vor allem darin, dass personenbezogene Daten

> „unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Anteilnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen."[89]

Das Grundrecht dient „unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung" der Absicherung der individuellen Selbstbestimmung.

> Diese setzt „voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[90]

Informationelle Selbstbestimmung ist als Grundlage der Freiheitsausübung auch Grundlage für die Ausübung weiterer Grundrechte.

> „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."[91]

Um vor diesen Gefährdungen zu schützen, gewährleistet

> das Grundrecht ... die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[92]

Jede Datenverarbeitung gegen den Willen der betroffenen Person ist daher ein *Eingriff* in die informationelle Selbstbestimmung.[93] Die Frage ob ein Eingriff vorliegt, ist nicht von der Person des Eingreifenden her zu bestimmen, sondern vom Schutzgut – der informationellen Selbstbestimmung – aus festzustellen. Daher kann es für die Eingriffsqualität grundsätzlich

---

89 *BVerfGE* 65, 1 (42).

90 *BVerfGE* 65, 1 (42f.).

91 *BVerfGE* 65, 1 (43).

92 *BVerfGE* 65, 1 (43).

93 S. *BVerfGE* 100, 313 (366); ebenso z.B. *Mallmann*, in: *Simitis u. a.*, BDSG, § 3 Rn. 106; *Walz*, in: *Simitis u. a.*, BDSG, § 4 Rn. 2; *Petersen* 2000, 31; auf eine untere Relevanzschwelle weist *Kunig*, Jura 1993, 601 hin; für eine restriktive Bestimmung des Schutzbereichs, um Kommuniktion nicht zu gefährden *Hoffmann-Riem*, AöR 1998, 527f.; grundsätzlich a.A. z.B. *Kloepfer* 1980, 23; *Gallwas*, NJW 1992, 2785, stellt nur auf die Gefährdung anderer Grundrechte ab und übersieht die eigene Qualität der informationellen Selbstbestimmung, wenn er feststellt, dass Datenverarbeitung als solche noch keine Freiheit beschneide.

keinen Unterschied machen, ob die Datenerhebung gegen den Willen der betroffenen Person von einer staatlichen Behörde oder einem privaten Unternehmen durchgeführt wird.[94] Die betroffene Person ist in beiden Fällen gleich schutzwürdig. Die Missachtung ihrer informationellen Selbstbestimmung ist in beiden Fällen ein Eingriff. Im Fall einer privatrechtlichen Offenbarungspflicht eines Entmündigten gegenüber seinem Vermieter hat das Bundesverfassungsgericht zutreffend festgestellt:

> „Nicht nur die öffentliche Bekanntmachung einer Entmündigung greift in das allgemeine Persönlichkeitsrecht ein, ..., sondern auch die Pflicht zur Offenbarung gegenüber einem Vertragspartner schränkt dieses Grundrecht ein."[95]

Eine davon zu unterscheidende Frage ist, welchen Schutz das Grundrecht auf informationelle Selbstbestimmung gegen diesen Eingriff gewährt und welche Verpflichtung für den Gesetzgeber zur Abwehr dieses Eingriffs besteht. In dieser Frage ist zu unterscheiden, dass das Grundrecht eine unmittelbare Abwehrfunktion nur gegenüber der staatlichen Gewalt begründet. Gegenüber anderen Privatpersonen begründet das Grundrecht dagegen keine unmittelbare Drittwirkung in Form eines Abwehrrechts.

Allerdings enthalten die Grundrechte nicht nur subjektive Abwehrrechte des Einzelnen gegen den Staat, sondern verkörpern „zugleich eine objektive Wertordnung", „die als verfassungsrechtliche Grundentscheidung für *alle Bereiche des Rechts* gilt und *Richtlinien und Impulse für Gesetzgebung*, Verwaltung und Rechtsprechung gibt".[96] Sie bilden zentrale Grundpfeiler einer gesellschaftlichen Ordnung:

> „Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. ... Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist."[97]

Eng mit dieser Aufgabenbestimmung durch die in den Grundrechten zum Ausdruck kommende Wertordnung ist die Verpflichtung des Gesetzgebers verbunden, sich schützend vor die Grundrechte zu stellen und eine Gewährleistungsfunktion für ihre Verwirklichung zu erfüllen.[98] Da gegenüber dem Staat bereits die Abwehrfunktion diese Aufgabe erfüllt, richtet sich die *Schutzaufgabe* des Gesetzgebers gegen private Dritte, die die Verwirklichung der informationellen Selbstbestimmung der betroffenen Person zu gefährden drohen.[99] Nach dieser Aufgabenbestimmung ist der Gesetzgeber verpflichtet, durch die einfachgesetzliche Aus-

---

94 Ebenso *Simitis*, NJW 1984, 401; *Hoffmann-Riem* 1997, 784; *ders.*, AöR 1998, 524; *Auernhammer* 1993, Einf. Rn. 12; § 1 Rn. 8f.; *Bizer* 1992, 297; *Mallmann*, CR 1988, 94; *Steinmüller*, DuD 1984, 94f.; *Wente*, NJW 1984, 1446f.; *Schlink*, DSt 1986, 245f.; *Tinnefeld/Ehmann* 1998, 91f.; *Schulz*, Verwaltung 1999, 143; *Kunig*, Jura 1993, 602; *Donos* 1998, 127, 49; a.A. z.B. *Kloepfer* 1980, 23: „verfassungswidrig"; *Zöllner*, RDV 1985, 12; *Krause*, JuS 1984, 268f.; *Ehmann*, RDV 1988, 169 ff.; 221 ff.

95 *BVerfGE* 84, 192 (195).

96 *BVerfGE* 39, 1 (41) - Hervorhebung durch die Verfasser.

97 *BVerfGE* 65, 1 (43).

98 Zur Ausgestaltung des Freiheitsbereichs zur Sicherung seiner Funktionsfähigkeit s. *Hoffmann-Riem*, AöR 1998, 523.

99 S. z.B. *Zöllner*, RDV 1985, 9; *Hoffmann-Riem*, AöR 1998, 5524; *Schulz*, Verwaltung 1999, 144 ff.; *Hoffmann-Rie*m 1997, 784, weist in diesem Zusammenhang auch auf die Privatisierungsfolgenverantwortung des Staats hin, wenn die für Informationsgesellschaft relevanten Infrastrukturen zunehmend von Privaten aufgebaut und betrieben werden.

gestaltung der Privatrechtsordnung die informationelle Selbstbestimmung des Einzelnen – insbesondere gegenüber der Informations- oder Wirtschaftsmacht Dritter – sicherzustellen.[100]

Für das Maß des Schutzes, das der Gesetzgeber zu gewährleisten hat, belässt das Grundgesetz einen weiten Ermessensspielraum.[101] Dieser wird nur durch das Untermaßverbot begrenzt.[102] Eine verfassungsrechtliche Handlungspflicht des Gesetzgebers besteht nur insoweit, als ohne den gesetzlichen Schutz das Grundrecht auf informationelle Selbstbestimmung in einem bestimmten Gesellschaftsbereich grundsätzlich gefährdet wäre.

4.2 Gleichbehandlung von öffentlichem und nicht öffentlichem Bereich

Die hier vorgeschlagene Regelung grundsätzlich gleicher Anforderungen an die Verarbeitung personenbezogener Daten im öffentlichen und nicht öffentlichen Bereich könnte gegen die Grundrechte der verantwortlichen Stellen verstoßen. Fordern die Grundrechte der Datenverarbeiter besondere Rücksichtnahme auf ihre Interessen und damit weniger strenge Anforderungen an die Datenverarbeitung in ihrem Bereich?[103] Einen grundsätzlichen Ausschluss der Gleichbehandlung würden diese Grundrechte aber als negative Kompetenzvorschriften nur dann fordern, wenn sie eine allein am Risikogehalt der Datenverarbeitung orientierte Regelung grundsätzlich ausschließen würden.[104] Der Umstand, dass einzelne Grundrechte durch einzelne Vorschriften berührt sind und eine Berücksichtigung erfordern, führt noch nicht zu einem grundsätzlichen Ausschluss der Gleichbehandlung. Die praktische Konkordanz zwischen der Schutzaufgabe für die informationelle Selbstbestimmung und dem Grundrecht der verantwortlichen Stelle kann in diesem Fall durch eine verhältnismäßige Ausgestaltung der Einzelregelung erreicht werden. Mit anderen Worten: Grundsätzlich gleiche Anforderungen an die Verarbeitung personenbezogener Daten im öffentlichen und nicht öffentlichen Bereich sind nur dann ausgeschlossen, wenn eine von der staatlichen Schutzaufgabe des Staats motivierte Regelung weniger Schutz für die informationelle Selbstbestimmung bieten müsste als eine an der Abwehrfunktion des Grundrechts gegenüber staatlicher Datenverarbeitung orientierte Regelung.

Für die Datenerhebung ist das Grundrecht auf *Informationsfreiheit*[105] nach Art. 5 Abs. 1 GG und für die Datenübermittlung das Grundrecht auf *Meinungsäußerungsfreiheit*[106] des Art. 5 Abs. 1 GG zu berücksichtigen.[107] Die Informationsfreiheit bietet jedoch keine Rechtsgrundlage für eine Erhebung personenbezogener Daten, die nicht auf eigener Wahrnehmung beruhen, nicht aus öffentlich zugänglichen Quellen stammen oder gar gegen den Willen der betroffenen Person gewonnen werden. Auch vermag sie nicht die Verarbeitung oder Übermittlung dieser Daten zu rechtfertigen. Die Informationsfreiheit endet, wo das berechtigte Abschir-

---

100 S. z.B. *Mallmann*, CR 1988, 94 ff.; *Hoffmann-Riem*, AöR 1998, 524; *Kloepfer* 1998, 68f., 95 und 111f.; *Schulz*, Verwaltung 1999, 145; zur Schutzpflicht für die wirtschaftliche Selbstbestimmung des Verbrauchers s. *Drexl* 1998, 258.

101 S. grundsätzlich *BVerfGE* 49, 89 (142); 56, 54 (78); zum Maß des Schutzes für die informationelle Selbstbestimmung s. z.B. *BVerfGE* 65, 1 (42 ff.); *Zöllner*, RDV 1985, 10; *Mallmann*, CR 1988, 94f.

102 S. *BVerfGE* 92, 26 (46).

103 So ausdrücklich *Kloepfer* 1980, 11f.; *Zöllner*, RDV 1985, 10; *Drews*, RDV 1987, 58 ff.

104 Eine getrennte Regelung fordert z.B. *Petersen* 2000, 49 ff, 153 ff.

105 S. z.B. *Gallwas*, NJW 1992, 2787.

106 Dieser Schutz wird überwiegend nur aufzählungsweise geltend gemacht - s. z.B. *Zöllner*, RDV 1985, 11; *Geis*, CR 1995, 172; *Kloepfer* 1980, 12; *Kloepfer* 1998, 94 – ausführlicher *Gallwas*, NJW 1992, 2785 ff.

107 S. z.B. *Schulz*, Verwaltung 1999, 148f.

mungsinteresse oder informationelle Selbstbestimmungsrecht eines anderen beginnt.[108] Regelungen, die der betroffenen Person die Autonomie über die Öffnung der Informationsquelle sichern, stellen keinen Eingriff in die Informationsfreiheit dar.[109] Hinsichtlich der Meinungsfreiheit ist zu berücksichtigen, dass es dem Informationsverarbeiter im Verhältnis zu anderen Personen möglich sein muss, sich durch eigene Wahrnehmung selbst ein Bild über eine Person zu machen und über dieses Bild auch mit anderen zu kommunizieren.[110] Die individuelle Meinungsbildung und der individuelle Meinungsaustausch, der zur Grundlage der Persönlichkeitsbildung gehört, ist somit durch Art. 5 Abs. 1 GG gedeckt.[111] Die Meinungsfreiheit ermöglicht, wahre Behauptungen über andere Personen aufzustellen und zu verbreiten.[112] Die Meinungsäußerungsfreiheit erstreckt sich jedoch nicht auf alle Phasen und Formen der automatischen Datenverarbeitung und selbst bei der Datenübermittlung nur auf die Übermittlungsvorgänge, die meinungsrelevant sind.[113] Zudem können beide Grundrechte durch allgemeine Gesetze, die sich wie Datenschutzregelungen nicht auf bestimmte Meinungen beziehen, eingeschränkt werden.[114] Eine gesetzliche Regelung, die den Auftrag zum Schutz der informationellen Selbstbestimmung risikobezogen umsetzt, ist daher auch im Geltungsbereich des Art. 5 GG zulässig, wenn sie die besondere Bedeutung der Informations- und Meinungsäußerungsfreiheit – ebenso wie die Mediengrundrechte und die Forschungsfreiheit – berücksichtigt.

Das Gleiche gilt auch für „die kommunikativen Komponenten" der Unternehmerfreiheit,[115] soweit sie als Bestandteile der *Freiheit der Berufsausübung* in Art. 12 Abs. 1 GG anerkannt sind. Auch diese so begründete Unternehmerfreiheit ermöglicht keinen Eingriff in Grundrechte Dritter. Umgekehrt können Anforderungen an die Datenverarbeitung oder gesetzlich zuerkannte Rechte betroffener Personen die Freiheit der Berufsausübung beeinträchtigen.[116] An die Berufsausübung können jedoch Anforderungen gestellt werden, wenn sie vernünftigen Erwägungen des Allgemeinwohls entsprechen. Gesetzliche Regelungen, die die Datenverarbeitung risikoorientierten Anforderungen unterwerfen, sind daher mit Art. 12 Abs. 1 GG vereinbar.[117] Allerdings müssen die Anforderungen im Einzelfall gerechtfertigt sein. Lässt zum Beispiel der Gesetzgeber auch Auskunftsansprüche zu, ohne das Geschäfts- und Betriebsgeheimnis zu schützen, indem er dieses als Ausschlussmerkmal vorsieht, kann dies einen unzulässigen Eingriff in die Freiheit der Berufsausübung des Art. 12 Abs. 1 GG darstellen.[118] Diese Schutzaspekte der Berufsfreiheit verhindern jedoch nicht eine gesetzliche Gleichbehandlung gleicher Risiken für die informationelle Selbstbestimmung im öffentlichen und nicht öffentlichen Bereich.

---

[108] S. z.B. *Hoffmann-Riem*, in: AK-GG, Art. 5 Rn. 91.; *Gallwas*, NJW 1992, 2787. Schon gar nicht begründet die Informationsfreiheit des Art. 5 Abs. 1 GG etwa einen Anspruch für Auskunfteien und Marketingunternehmen, sich über das Recht auf informationelle Selbstbestimmung hinwegzusetzen – s. z.B. *Simitis*, in: *ders. u.a.*, BDSG, § 1 Rn. 191f.; *Podlech/Pfeiffer*, RDV 1998, 143.

[109] S. z.B. *Schulz*, Verwaltung 1999, 149.

[110] Der Einzelne hat kein allgemeines und umfassendes Verfügungsrecht über die Darstellung der eigenen Person. Insbesondere vermittelt das allgemeine Persönlichkeitsrecht dem Einzelnen nicht den Anspruch, nur so von anderen dargestellt zu werden, wie er sich selbst sehe oder gesehen werden möchte – s. *BVerfGE* 101, 361 (380) unter Hinweis auf *BVerfGE* 82, 236 (269); 97, 125 (149); 97, 391 (403); 99, 185 (194).

[111] S. z.B. *Gallwas*, NJW 1992, 2787f.

[112] S. *BVerfGE* 99, 185 (196); *BVerfG*, AfP 2000, 447 ff.

[113] S. z.B. *Schulz*, Verwaltung 1999, 139f.

[114] S. z.B. *Petersen* 2000, 93. Außerdem sind Regelungen zulässig, die Konflikte mit anderen Grundrechten ausgleichen – s. z.B. *Schultze-Fielitz*, in: *Dreier*, GG, Art. 5 Rn. 121.

[115] S. z.B. *Zöllner*, RDV 1985, 11; *Kloepfer* 1980, 12; *Geis*, CR 1995, 172.

[116] S. z.B. *Schulz*, Verwaltung 1999, 147.

[117] S. z.B. *Schulz*, Verwaltung 1999, 148.

[118] S. z.B. auch *Drexl* 1998, 251.

Ähnliches gilt für den Schutz der Datenverarbeitung durch das Grundrecht auf *Eigentum*. Dieser erstreckt sich nur auf das Erworbene, nicht auf die Tätigkeit des Erwerbens.[119] Er gilt daher allenfalls für Datenträger oder Datenverarbeitungssysteme und die auf ihnen befindlichen Datensammlungen.[120] Das Grundrecht gibt keinen Anspruch auf die Verarbeitung personenbezogener Daten gegen oder ohne den Willen der betroffenen Person. Selbst hinsichtlich des geschützten Umfangs verhindert das Grundrecht kein Gesetz, durch das die Eigentumsordnung in der Form ausgestaltet wird, dass die Nutzung von Eigentum keine Grundrechte Dritter beeinträchtigt.

Die *wirtschaftliche Betätigungsfreiheit* als Unterfall der allgemeinen Handlungsfreiheit nach Art. 2 Abs. 1 GG wird von manchen als die eigentliche Grundlage des Grundrechtsschutzes des Datenverarbeiters angesehen.[121] Hieraus wird eine Unternehmerfreiheit zur Datenverarbeitung abgeleitet:[122] Aus dieser folge, dass der Gesetzgeber die Rechtskreise der Beteiligten so gegeneinander abgrenzen müsse, dass jeder seine Teilnahme am Privatrechtsverkehr gestalten könne, ohne ständig Gefahr zu laufen, Rechte anderer zu beeinträchtigen. Beziehungen zwischen Privaten könnten ihren Ausgangspunkt daher nicht in unbegrenzter, sondern nur in „gegenständlich verkörperter Freiheit“ finden.[123] Entsprechend den Grundsätzen des allgemeinen Persönlichkeitsrechts sei der Geheimhaltungswille des Betroffenen nur dann zu berücksichtigen, wenn dieser sich deutlich durch eine Erklärung manifestiert habe oder gesetzlich anerkannt sei.[124] Ausgangspunkt aller gesetzgeberischen Überlegungen müssten daher die Freiheit zur Datenverarbeitung, nicht ihre Beschränkung sein.[125] Dieser Meinung kann jedoch nicht gefolgt werden: Das Grundrecht auf informationelle Selbstbestimmung beschränkt sich nicht auf nach außen kenntlich gemachte Geheimnisse, sondern begründet einen Entscheidungsvorrang der betroffenen Person über die Daten, die sich auf ihre sachlichen und persönlichen Verhältnisse beziehen. Umgekehrt steht die geltend gemachte allgemeine Handlungsfreiheit unter dem Vorbehalt der verfassungsmäßigen Ordnung und der Rechte Dritter. Sie endet, wo das berechtigte Abschirmungsinteresse oder informationelle Selbstbestimmungsrecht eines anderen beginnt.[126] Sie kann sich – von zu berücksichtigenden Ausnahmen abgesehen[127] – grundsätzlich nur auf die Verarbeitung personenbezogener Daten erstrecken, denen die betroffene Person zugestimmt hat. Datenschutzrechtliche Regelungen sind als Teil der verfassungsmäßigen Ordnung gerechtfertigt.[128]

Im Ergebnis werden dem Gesetzgeber durch die Grundrechte der verantwortlichen Stellen keine grundsätzlichen Einschränkungen für die Ausgestaltung der Informationsordnung hinsichtlich personenbezogener Daten auferlegt. Insbesondere ist er nicht daran gehindert, für den öffentlichen und den nicht öffentlichen Bereich das gleiche Datenschutzniveau zu fordern und für beide Bereiche im Prinzip gleiche Grundsätze zur Anwendung zu bringen.[129] Die

---

119 Diese ist allein durch Art. 12 Abs. 1 GG geschützt - s. z.B. *BVerfGE* 30, 292 (335).

120 S. z.B. *Petersen* 2000, 109.

121 S. z.B. *Zöllner*, RDV 1985, 11; *Kloepfer* 1980, 12; *Geis*, CR 1995, 172. *Gallwas*, NJW 1992, 2786, legt das Schwergewicht mehr auf die Informationsaufnahme und Kommunikation, die für die persönliche Entfaltung in einer Gesellschaft erforderlich ist.

122 S. z.B. *Kloepfer* 1980, 12; *Zöllner*, RDV 1985, 4 ff.; *Schmitt Glaeser* 1989, 93; *Breitfeld* 1992, 18 ff.; *Büser*, BB 1997, 213 ff.

123 S. z.B. *Ehmann*, AcP 1988, 251, 304 ff.; *Breitfeld* 1992, 37, 115; *Büser*, BB 1997, 215.

124 S. z.B. *Breitfeld* 1992, 115; *Büser*, BB 1997, 215; nur in diesem Umfang wird dann auch ein berechtigtes Interesse der betroffenen Person anerkannt – s. z.B. *Büser*, BB 1997, 217.

125 S. z.B. auch *Schmitt Glaeser* 1989, 91.

126 S. z.B. *Hoffmann-Riem*, in: AK-GG, Art. 5 Rn. 91; *Gallwas*, NJW 1992, 2787.

127 S. Teil 3 Kap. 3.1.4.

128 S. z.B. *Schulz*, Verwaltung 1999, 150.

129 Ebenso *Mallmann*, CR 1988, 95.

Grundrechte der verantwortlichen Stellen fordern keine grundsätzlich unterschiedliche Behandlung.

Umgekehrt fordern die informationelle Selbstbestimmung und die sie verstärkenden Grundrechte[130] ein am Schutzbedarf orientiertes Datenschutzniveau. Wenn von der Datenverarbeitung im nicht öffentlichen Bereich eine vergleichbare – oder inzwischen sogar eine größere – Gefährdung für die informationelle Selbstbestimmung und die anderen Grundrechte der betroffenen Person ausgeht,[131] dann fordert der Schutz dieser Grundrechte ein vergleichbares oder sogar ein höheres Datenschutzniveau im nicht öffentlichen Bereich.

Der Gesetzgeber hat die Grenze zwischen beiden Grundrechtsbereichen festzulegen, ohne dass dabei prinzipiell ein Vorrang oder ein Anspruch der Datenverarbeiter auf die Verarbeitung personenbezogener Daten Dritter besteht.[132] Zwischen den Grundrechten der Datenverarbeiter und den Grundrechten der betroffenen Personen besteht *keine strukturell gleiche* Situation für die Verwirklichung der jeweiligen Grundrechte, deren Gleichheit einen im Weg des gleichermaßen beiderseitigen Nachgebens[133] zu findenden Interessenausgleich erforderte.[134] Vielmehr ist für die Abgrenzung der Grundrechtsbereiche vom Grundsatz her zu berücksichtigen, dass das Recht auf informationelle Selbstbestimmung ein defensives Abwehrrecht ist,[135] während die Behauptung eines Grundrechts auf Datenverarbeitung einen Anspruch geltend macht, aggressiv in die Grundrechtssphäre Dritter einzugreifen.[136] Einen solchen Anspruch enthalten die Grundrechte jedoch nicht. Vielmehr ist es Aufgabe des Gesetzgebers, konkurrierende Grundrechtssphären so abzugrenzen, dass die Ausübung von Grundrechten nicht dazu führt, dass dadurch in die Grundrechte anderer eingegriffen wird. Soweit der Gesetzgeber nicht das Grundrecht auf informationelle Selbstbestimmung zugunsten überwiegender öffentlicher oder privater Interessen durch Gesetz eingeschränkt hat,[137] haben auch Private kein eigenständiges Recht zur Verarbeitung personenbezogener Daten Dritter.[138]

Wenn schon dem Staat selbst im öffentlichen Interesse nicht ohne weiteres erlaubt ist, in Grundrechte der Bürger einzugreifen, gilt dies erst recht für privatwirtschaftliche Unternehmen, die nicht aus öffentlichen, sondern aus kommerziellen Interessen handeln.[139] Für konkurrierende Privatinteressen muss vielmehr gelten, dass sie grundsätzlich gleichrangig sind.[140] In der auf Willensübereinstimmung und Gleichheit zielenden Privatrechtsordnung muss die grundsätzliche Gleichwertigkeit der Parteien gewährleistet sein. Das adäquateste und geeig-

---

130 S. zu diesen Teil 3 Kap. 1.

131 S. Teil 1 Kap. 2.1 und 2.2.

132 S. z.B. *Gallwas*, NJW 1992, 2785 ff.

133 Dies ist nicht einmal *nach* der gesetzlichen Anerkennung von Rechten der Datenverarbeitung gefordert – s. *BVerfGE* 84, 192 (195).

134 So aber z.B. *Zöllner*, RDV 1985, 11; *Kloepfer* 1980, 13; *Kloepfer* 1998, 78f.

135 Die aktiven Ansprüche der betroffenen Person auf Auskunft, Berichtigung, Sperrung, Löschung und Widerspruch sind Folgeansprüche aufgrund der Ingerenz des Datenverarbeiters.

136 Zu recht weist der *BGH*, BB 1999, 1131, darauf hin, dass der Schutz der Individualsphäre vorrangig gegenüber dem wirtschaftlichen Gewinnstreben von Wettbewerbern ist und dass die berechtigten Interessen der gewerblichen Wirtschaft, ihre Produkte werbemäßig anzupreisen, es angesichts der Vielfalt der Werbemethoden nicht erfordern, mit Werbemaßnahmen auch in den privaten Bereich des umworbenen Verbrauchers einzudringen.

137 Durch eine solche verhältnismäßige Zuordnung der Grundrechtsbereiche durch den Gesetzgeber kann z.B. das berechtigte Interesse von Gläubigern, das Investitionsrisiko durch Schuldnerverzeichnisse oder branchenbezogene Warndienste zu begrenzen, zur Geltung gebracht werden.

138 Im Ergebnis ebenso *Simitis*, in: *ders. u.a.*, BDSG, § 1 Rn. 192; *Geis*, CR 1995, 172.

139 S. z.B. *Gola/Schomerus*, § 29 Anm. 4.7; *Wittig*, RDV 2000, 61.

140 S. *Podlech/Pfeiffer*, RDV 1998, 144.

netste Mittel, eine Gleichordnung herzustellen, ist eine kongruente Interessenübereinstimmung, die durch einen Vertrag oder eine Einwilligung herbeigeführt wird.[141] Umgekehrt zur Behauptung eines Datenverarbeitungsrechts ist es richtig, dass nach dem im Privatrecht überall herrschenden Prinzip der Willensfreiheit und der Vertragsbindung ein Recht zur Verarbeitung personenbezogener Daten vom Grundsatz her nur dann begründet werden kann, wenn hierüber zwischen den Beteiligten Einverständnis erzielt worden ist.[142]

Wenn unterschiedliche Lösungen privatrechtlicher und öffentlich rechtlicher Interessenkonflikte mit einer situationsgerechten Anwendung der Grundrechte begründet und geringere Anforderungen an den Datenschutz im privatrechtlichen Bereich früher vor allem mit der geringeren Gefährdung der Interessen Betroffener in diesem Bereich begründet wurde,[143] dann muss sich dieses Ergebnis in dem Maß wandeln, in dem die Risiken der privaten Verarbeitung personenbezogener Daten zugenommen haben.[144] Wenn von diesen inzwischen die größere Bedrohung auszugehen scheint,[145] müssen auch einer situationsgerechten Anwendung der Grundrechte entsprechend die Anforderungen an die privatwirtschaftliche Datenverarbeitung eher höher sein als die für den öffentlichen Bereich. Hier ist an den zentralen Kern der Drittwirkungslehre zu erinnern:

> „Menschliche Freiheit ist nicht nur durch den Staat, sondern auch durch nichtsstaatliche Mächte gefährdet, die in der Gegenwart bedrohlicher werden können als die Gefährdungen durch den Staat. Freiheit lässt sich jedoch wirksam nur als einheitliche gewährleisten: sofern sie nicht nur eine Freiheit der Mächtigen sein soll, bedarf sie des Schutzes auch gegen gesellschaftliche Beeinträchtigungen.“[146]

Je mehr die Datenverarbeitung mit der Ausübung wirtschaftlicher und sozialer Macht verbunden ist, desto wirksamer müssen die rechtlichen Schutzvorkehrungen zugunsten des Einzelnen sein.[147] Der Gesetzgeber ist jedenfalls durch die Grundrechte der Datenverarbeiter nicht daran gehindert, allgemeine auch für sie geltende Datenschutzgrundsätze aufzustellen.

Dieses Ergebnis bedeutet nicht, dass die jeweils einschlägigen Grundrechte verantwortlicher Stellen für das künftige Datenschutzrecht bedeutungslos wären. Vielmehr muss der Gesetzgeber neben der informationellen Selbstbestimmung als Grundrecht der betroffenen Person und als Leitprinzip der gesetzlichen Ausgestaltung einer gesellschaftlichen Informations- und Kommunikationsordnung auch die Grundrechte der verantwortlichen Stellen berücksichtigen. Dies wird im Folgenden dort berücksichtigt, wo dies im Einzelfall erforderlich erscheint.

4.3 Bestimmtheit und Normenklarheit gesetzlicher Erlaubnistatbestände

Bei der Ausgestaltung der Struktur des künftigen Datenschutzrechts ist der Gesetzgeber weitgehend frei, was die Rechte der betroffenen Person, die technisch-organisatorischen Anforderungen, die Vorgaben zur Auditierung und Zertifizierung, die Rahmensetzung für die

---

141 *Podlech/Pfeiffer*, RDV 1998, 145.

142 S. hierzu auch *Bizer*, DuD 1999, 552.

143 S. z.B. *Bühnemann*, BB Beilage zu Heft 3/1974, 4; *Kloepfer* 1980, 10 ff.; *Zöllner*, RDV 1985, 8, 10. Daneben wurde auf die Rolle des Datenverarbeiters als Grundrechtsträger verwiesen.

144 Ebenso *Mallmann*, CR 1988, 94.

145 S. Teil 1 Kap. 2.1 und die dortigen Nachweise; dies sehen zum Teil auch diejenigen Autoren, die früher das Gegenteil vertraten – s. z.B. *Kloepfer* 1998, 68f: „Die Datenschutzhölle – das sind heute vor allem die anderen; der Überwachungsnachbar und -konkurrent scheint zu drohen“, oder: „Die Aktivitäten etwa der großen Informationsdienstleister, aber auch die Tätigkeiten der Kreditauskunftsunternehmen ... sind für die Existenz des Einzelnen nicht selten sehr viel bedeutsamer als viele behördliche Datenverarbeitungen“, oder: „Tatsächlich verfügen internationale Datenverarbeitungs-Dienstleister heute schon über wesentlich tiefere Einblicke in die Privatsphäre vieler Menschen als behördliche Datensammlungen.“

146 *Hesse* 1995, Rn. 349.

147 *Mallmann*, CR 1988, 95.

Selbstregulierung, die Datenschutzkontrolle sowie die Anforderungen an die Transparenz der Datenverarbeitung, an den System- und den Selbstschutz, an die Vermeidung des Personenbezugs und die Datensicherheit angeht. Soweit er das Grundrecht auf informationelle Selbstbestimmung einschränkt, hat er jedoch folgende Vorgaben des Bundesverfassungsgerichts zu beachten:

> „Diese Beschränkungen bedürfen nach Art. 2 Abs. 1 GG ... einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht.[148] Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten", nach dem Grundrechte „von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerlässlich ist.[149] Angesichts der ... Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."[150]

Für allgemeine einschränkende Regelungen des Datenschutzrechts gibt das Bundesverfassungsgericht die anzustrebende „Normenklarheit" als Ziel vor. Das Gebot der Normenklarheit fordert, dass die Regelung so klar gefasst sein muss, dass die betroffene Person erkennen kann, unter welchen Voraussetzungen und inwieweit ihr Recht auf informationelle Selbstbestimmung eingeschränkt wird.[151] Mit welchen Mitteln der Gesetzgeber die Normenklarheit erzielt, wird ihm überlassen. Zur Erfüllung dieser Vorgabe zählt letztlich nur das Ergebnis. Wenn mit der empfohlenen Neukonzeption dieses Ergebnis verbessert wird, kann dies in keinem Fall gegen die Anforderung des Bundesverfassungsgerichts verstoßen.

Allein für die Regelung von Erlaubnistatbeständen zur zwangsweisen Erhebung und Verwendung personenbezogener Daten stellt das Bundesverfassungsgericht zur Festlegung der Verarbeitungszwecke weitere Anforderungen:

> „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind."[152]

Durch die Notwendigkeit einer bereichsspezifischen und präzisen gesetzlichen Bestimmung des Verwendungszwecks könnte die empfohlene Umkehrung des Verhältnisses von allgemeinem BDSG zu den bereichsspezifischen Datenschutzregelungen mit dem Ziel, diese weitgehend zu reduzieren, für die Erlaubnistatbestände in Frage gestellt sein.

Allerdings stellt das Bundesverfassungsgericht diese Forderung nicht ohne Ausnahme auf, sondern erkennt bereichsspezifische Besonderheiten an und reagiert auf diese flexibel. So stellt es fest, dass zum Beispiel „für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden" kann. Es akzeptiert in diesem Bereich ein „Bedürfnis nach Vorratsspeicherung" und macht eine Ausnahme vom strikten Verbot der Sammlung personenbezogener Daten auf Vorrat.[153]

Die Forderung nach einer bereichsspezifischen und präzisen gesetzlichen Bestimmung des Verwendungszwecks ist jedoch kein Selbstzweck, sondern soll den Gesetzgeber zwingen, sich mit den Risiken der konkreten Verarbeitungsbedingungen und -zwecke eines bestimmten Verwaltungsbereichs auseinanderzusetzen und spezifische und angepasste Regelungen für

---

148 Hier verweist das *BVerfG* auf *BVerfGE* 45, 400 (420).

149 Hier verweist das *BVerfG* auf *BVerfGE* 19, 342 (348).

150 *BVerfGE* 65, 1 (44) unter Verweis auf *BVerfGE* 53, 30 (65); 63, 131 (143).

151 *BVerfGE* 65, 1 (44); *Petersen* 2000, 32f.

152 *BVerfGE* 65, 1 (46).

153 *BVerfGE* 65, 1 (47).

diese zu treffen.[154] Die Bestimmung der Mittel bereichsspezifischer und präziser Zweckfestlegung, um dieses Ziels zu erreichen, war vom Bundesverfassungsgericht nicht als Formalismus gemeint, sondern als risikobezogene Reaktion auf die Erkenntnis, dass für die grundrechtliche Bedeutung der Datenverarbeitung in erster Linie der Verarbeitungszweck und der Verwendungskontext entscheidend sind.

Das vom Bundesverfassungsgericht mit dieser Forderung verfolgte Ziel, eine für den jeweiligen Verwendungszweck spezifische risikoadäquate Regelung zu erzwingen, wurde weitgehend verfehlt.[155] Das überwiegende Ergebnis dieser Forderung ist der Nachvollzug der Datenverarbeitungspraxis durch eine Normenflut bereichsspezifischer Regelungen. Diese sind bisweilen ähnlich allgemein wie die allgemeinen Erlaubnistatbestände im BDSG, bisweilen aber auch überdetailliert und sogar von einer perfektionistischen Präzision. Dennoch enthalten sie selbst in diesen Fällen eine zusätzliche Generalklausel, um die Fülle tatsächlicher Verwendungszwecke regulativ einzufangen. Im Ergebnis führt die Forderung einer bereichsspezifischen und präzisen gesetzlichen Bestimmung des Verwendungszwecks bei der „unendlichen" Vielzahl von Verwaltungszwecken und Verwendungsbedingungen moderner Datenverarbeitung zu einem direkten Widerspruch mit der Forderung nach Normenklarheit der Erlaubnistatbestände.[156]

Das Bundesverfassungsgericht kann diese negativen Folgen der Umsetzung seiner Forderung nicht gewollt haben.[157] Seine Forderung nach einer bereichsspezifischen und präzisen gesetzlichen Bestimmung des Verwendungszwecks muss daher auf ihr grundlegendes Ziel bezogen und neu operationalisiert werden.[158] Entscheidend an der Forderung des Gerichts ist einmal, dass nicht die verantwortliche Stelle über neue Verarbeitungszwecke und -möglichkeiten entscheidet, sondern der Gesetzgeber. Zum Anderen ist wichtig, dass dieser seine Entscheidung über die Einschränkung des Grundrechts auf informationelle Selbstbestimmung an dessen Gefährdung ausrichtet. Notwendig ist also eine risikoorientierte Interpretation der Forderung des Bundesverfassungsgerichts.[159]

Danach muss es dem Gesetzgeber möglich sein, den Allgemeinheits- oder Spezialisierungsgrad seiner Regelung nach der Gefährdung der informationellen Selbstbestimmung zu differenzieren.[160] Um die Klarheit und Verständlichkeit der Datenschutzrechtsordnung zu wahren, muss es ihm möglich sein, normale Risiken durch die heutzutage übliche Datenverarbeitung in durchschnittlichen Verwaltungszweigen durch allgemeine Regelungen zuzulassen und diese Regelungen in einem allgemeinen Gesetz „vor die Klammer zu ziehen".[161] Gemeint sind damit Regelungen, die heute ohnehin alle im Wesentlichen den gleichen Wortlaut haben und für die sich die bereichsspezifische Regelung weitgehend als bloßer Formalismus erweist.[162]

---

154 S. hierzu z.B. *Simitis* 1990, 484 ff.

155 S. hierzu näher Teil 1 Kap. 2.4 m.w.N.

156 S. hierzu z.B. auch *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7 Rn. 18f.; *Bull*, RDV 1999, 148f.; *ders.* 1998, 25; *Petersen* 2000, 113; *Bäumler*, DuD 1997, 446; s. auch *Zuck*, NJW 1999, 1517 ff.

157 *Hoffmann-Riem* 1997, 782, stellt sogar fest, dass die bisherige Strategie der Verrechtlichung einen effektiven Datenschutz leerlaufen lässt.

158 *Hoffmann-Riem*, AöR 1998, 527f. will sogar weitergehend den Schutzbereich des informationellen Selbstbestimmung zu diesem Zweck restriktiv interpretieren. Für die Gesetzgebung zieht er den Schluss: „Ohne Beschränkung auf den Schutz vor erheblichen Risiken droht der Auftrag zur Sicherung einer funktionsfähigen, d.h. aber auch nutzbaren, kommunikativen Infrastruktur verfehlt zu werden." Für eine restriktive Interpretation des Volkszählungsurteils auch *Petersen* 2000, 129.

159 Ebenso *Hoffmann-Riem* 1997, 782.

160 So auch *Hoffmann-Riem*, AöR 1998, 528.

161 S. hierzu auch *Bull*, RDV 1998, 152.

162 S. dazu *Bäumler/v. Mutius* 1999.

Sollen dagegen überdurchschnittliche Eingriffe in die informationelle Selbstbestimmung durch besonders invasive Zwecke oder Mittel erlaubt werden, ist eine bereichsspezifische und präzise Regelung der zulässigen Zwecke und Mittel erforderlich.[163] In diesen Fällen ist es erforderlich, dass die bereichsspezifischen Gesetze Ausnahmen in Form von Verschärfungen gegenüber den allgemeinen Regelungen enthalten.[164]

Diese risikoorientierte Interpretation der Forderung des Bundesverfassungsgerichts nach einer bereichsspezifischen und präzisen gesetzlichen Bestimmung des Verwendungszwecks wendet im Grunde nur den Grundsatz der Verhältnismäßigkeit auf diese Forderung selbst an[165] und gelangt damit zu einem die Nachteile seiner bisherigen Umsetzung vermeidenden und die Vorteile sichernden Ergebnis. Dem Anliegen des Bundesverfassungsgerichts wird besser entsprochen, wenn „dem Perfektionsstreben der Vergangenheit abgeschworen" wird, eine Konzentration auf die wirklichen Risiken erfolgt und die Effektivität des Datenschutzrechts dadurch letztlich gesteigert wird.[166]

5. Europarechtliche Zulässigkeit der Neukonzeption

Die Datenverarbeitung für den öffentlichen und den nicht öffentlichen Bereich grundsätzlich einheitlich zu regeln, entspricht der Konzeption der Datenschutzrichtlinie, die ebenfalls nicht zwischen beiden Bereichen differenziert.[167]

Die Neukonzeption des Verhältnisses zwischen allgemeinen und bereichsspezifischen Regelungen widerspricht ebenfalls nicht der Datenschutzrichtlinie. Diese enthält in Art. 7 DSRL zwar einen Regelungsvorbehalt für Erlaubnistatbestände, aber keine Vorgaben über die Regelungstiefe[168] oder die Verteilung der Regelungen auf unterschiedliche Gesetze.[169] Sie überlässt es dem nationalen Gesetzgeber, ob er ein allgemeines Gesetz zum Schutz von Personen bei der Datenverarbeitung oder für bestimmte Bereiche jeweils eigene Regelungen schafft.[170] Ohnehin ist der Regelungsumfang und die Regelungsdichte des deutschen Datenschutzrechts in der Europäischen Gemeinschaft einzigartig.

Die in Teil 3 empfohlene Neukonzeption sieht zur Fortentwicklung des Datenschutzrechts teilweise Regelungen vor, die über das Datenschutzniveau der Datenschutzrichtlinie hinausgehen. Daher stellt sich die Frage, ob die Mitgliedstaaten über den in der Richtlinie festgeschriebenen Standard hinausgehen dürfen oder ob dieser die „Obergrenze" zulässiger nationaler Regelungen bildet.

Über die Spielräume, die das Regulierungsinstrument der Richtlinie den Mitgliedstaaten nach Art. 249 Abs. 3 EGV in der Wahl der Mittel zur Umsetzung des verbindlichen Ziels lässt, hinaus gewährt die Datenschutzrichtlinie zusätzliche Entscheidungsspielräume. Nach Art. 5 DSRL sollen die Mitgliedstaaten die Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, „nach Maßgabe" der Art. 6 bis 21 DSRL näher bestimmen. Die Datenschutzrichtlinie gibt somit nur einen Rahmen vor, der vom nationalen

---

163 Dies entspricht der von mehreren Autoren vertretenen „Schwellentheorie" – s. z.B. *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1 Rn. 65; *Simitis*, in: *ders. u.a.*, BDSG, § 1 Rn. 197; *Dammann*, in: *Simitis u.a.*, BDSG, § 14 Rn. 2 jeweils m.w.N.; s. hierzu auch *Petersen* 2000, 144.

164 S. hierzu Teil 2 Kap. 3.1 und Teil 3 Kap. 3.1.3.

165 Die Begrenzung der rechtlichen Regulierung auf das Erforderliche fordert auch *Hoffmann-Riem*, AöR 1998, 526 ff.

166 S. *Bull*, RDV 1998, 148.

167 S. z.B. *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 6 Rn. 6; *Simitis*, NJW 1997, 287; *Garstka*, DVBl 1998, 985; *Petersen* 2000, 60.

168 S. z.B. *Dammann/Simitis*, Art. 5 Rn. 1.

169 S. z.B. *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 5 Rn. 6; *Weber*, CR 1995, 298.

170 S. Erwägungsgrund 23; s. auch *Petersen* 2000, 69.

Gesetzgeber ausgefüllt werden kann. Durch diese bewusst offene Gestaltung nimmt die Datenschutzrichtlinie Rücksicht auf die unterschiedlichen Rechtskulturen und -traditionen der einzelnen Mitgliedstaaten und die daraus resultierende Vielfalt an Lösungsmöglichkeiten und differenzierenden Wertungen.[171]

Die Datenschutzrichtlinie zwingt nicht, das bisher unterschiedliche Datenschutzniveau in den Mitgliedstaaten einzuebnen. Vielmehr bestimmt Erwägungsgrund 10, dass die Angleichung der Rechtsvorschriften „nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen" darf, im Gegenteil muss sie „darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen". Soweit nationale Rechtsvorschriften, wie zumindest teilweise das deutsche Datenschutzrecht für den öffentlichen Bereich, bereits ein Datenschutzniveau erreicht haben, das über dem der Richtlinie liegt, müssen sie dieses hohe Schutzniveau beibehalten.[172] Diese „Öffnung nach oben" bietet die Richtlinie aber nicht nur für das bei ihrem Inkrafttreten geltende nationale Recht, sondern auch für dessen Fortentwicklung.[173] Ausdrücklich fordert Erwägungsgrund 9 die Mitgliedstaaten auf, innerhalb des durch die Richtlinie gewährten Spielraums „eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes" anzustreben.[174] „Korrekturen scheinbar festgefügter, von der Richtlinie kritiklos übernommener Grundsätze sind daher ebenso möglich wie eine ‚Modernisierung' des Datenschutzes."[175] Unterschiede, die dadurch bei der Durchführung der Richtlinie entstehen, nimmt die Richtlinie hin, selbst wenn dies „Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann".[176]

Im Ergebnis ist daher festzuhalten, dass die Datenschutzrichtlinie kein prinzipielles Hindernis für eine Fortentwicklung des deutschen Datenschutzrechts darstellt, allerdings dürfen die Regelungen im Einzelnen nicht gegen den von der Richtlinie vorgegebenen Rahmen verstoßen.

Hier sind insbesondere die Regelungen zur Zulässigkeit der Datenverarbeitung in Art. 6, 7 und 8 DSRL zu beachten. Die Regelungen zur Datenverarbeitung in Art.6 DSRL und die Regelungen zu besonders schützenswerten Daten in Art. 8 DSRL bieten ihrem Wortlaut nach nur einen Gestaltungsspielraum bei der Präzisierung der verwendeten Begriffe. Beispielsweise fordert der Wortlaut des Art. 8 Abs. 2 und 3 DSRL („findet keine Anwendung") eine Übernahme der Erlaubnistatbestände.[177] Dagegen bietet Art. 7 DSRL einen größeren Gestaltungsspielraum. Diese Vorschrift besagt, dass eine Verarbeitung personenbezogener Daten „lediglich erfolgen darf", wenn eine der in der Vorschrift genannten Voraussetzungen erfüllt ist. Sie verhindert damit zusätzliche Erlaubnistatbestände, fordert aber nicht, dass der

---

171 S. z.B. *Weber*, CR 1995, 298; *Dammann/Simitis*, Art. 5 Rn. 1; *Kloepfer* 1998, D 105, 115; *Petersen* 2000, 68.

172 S. z.B. *Weber*, CR 1995, 298; *Simitis*, NJW 1998, 2476; *ders.*, DuD 2000, 714f.

173 Nach *Simitis* ist jeder Mitgliedstaat sogar verpflichtet, nicht nur sämtliche Chancen zu nutzen, die sich aus der Richtlinie ergeben, den Datenschutz auszubauen, sondern zusätzlich gehalten, die Defizite der Richtlinie durch eigene Vorschriften zu korrigieren – s. *Dammann/Simitis* 1997, Einl. Rn. 10; *Simitis*, NJW 1997, 282; *ders.*, NJW 1998, 2476; *ders.*, DuD 2000, 714f. Abweichungen „nach oben" halten auch für zulässig *Jacob*, RDV 1993, 11; *Lütkemeier*, DuD 1995, 598.

174 „Harmonisierung" kann somit allenfalls einen gemeinsamen Ausgangs-, nicht aber einen, sei es auch nur vorläufigen Endpunkt der Regelungsanstrengungen fixieren – *Dammann/Simitis* 1997, Einl. Rn. 9; *Simitis*, DuD 2000, 714f.

175 *Simitis*, NJW 1998, 2476; s. auch *ders.*, DuD 2000, 714f.

176 Ohne auf diesen Erwägungsgrund einzugehen interpretiert *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 5 Rn. 7 die Richtlinie als „abschließende Vollharmonisierung"; ähnlich *Geis*, DuD 1995, 177.

177 S. z.B. *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 8 Rn. 6.

nationale Gesetzgeber die in Art. 7 DSRL genannten Erlaubnistatbestände ausschöpft.[178] Daher ist es kein Verstoß gegen die Datenschutzrichtlinie, wenn beispielsweise die Erlaubnis der Datenverarbeitung zur Verwirklichung eines berechtigten Interesses nicht generell übernommen wird, sondern die Interessen, die eine Datenverarbeitung auch gegen den Willen der betroffenen Person erlauben sollen, einengend und präziser festgelegt werden.[179]

Weitere spezifische Vorgaben der Datenschutzrichtlinie werden bei der Erörterung einzelner Regelungsvorschläge berücksichtigt.

Für jede Modernisierung des nationalen Datenschutzrechts ist aber grundsätzlich zu beachten, dass die Einführung eines in der Gemeinschaft einheitlichen datenschutzrechtlichen Niveaus den Zweck hat, die Hindernisse für den freien Verkehr personenbezogener Daten zu beseitigen, die bislang durch Unterschiede im geltenden Recht der Mitgliedstaaten bedingt waren.[180] Die Richtlinie geht davon aus, dass sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ein gleichwertiger Schutz in der Gemeinschaft ergibt, der einen freien Verkehr der Daten ermöglicht.[181] Daher verpflichtet Art. 1 Abs. 2 DSRL die Mitgliedstaaten, auf besondere Schranken des innergemeinschaftlichen Verkehrs personenbezogener Daten zu verzichten. Dies bedeutet, dass jeder Mitgliedstaat die Regelungen zur Umsetzung der Richtlinie in anderen Mitgliedstaaten anerkennen muss, auch wenn diese sich von den eigenen Regelungen unterscheiden und vielleicht nicht das gleiche Schutzniveau erreichen.[182]

Für den grenzüberschreitenden Datenverkehr innerhalb Europas bedeutet dies: Der Import von Daten darf nicht behindert werden, auch wenn die in einem anderen Mitgliedstaat vorgenommene Übermittlung nicht den inländischen Rechtsanforderungen entspricht. Dagegen gelten diese für darauffolgende Verarbeitungen durch inländische verantwortliche Stellen ohne Unterschied nach der Herkunft der Daten. Der Export von personenbezogenen Daten in andere Mitgliedstaaten darf ebenfalls nicht durch weitergehende nationale Regelungen behindert werden. Von Bedeutung ist diese Garantie des freien Warenverkehrs personenbezogener Daten vor allem bei grenzüberschreitenden Verarbeitungen, die von einer in einem anderen Mitgliedstaat niedergelassenen verantwortlichen Stelle nach den Rechtsvorschriften dieses Mitgliedstaats in Deutschland vorgenommen werden.[183] Diese Vorgaben sind durch Übermittlungsregelungen, wie sie in § 4a und b BDSG enthalten sind, zu berücksichtigen.[184]

6. Aufnahme der informationellen Selbstbestimmung ins Grundgesetz

Die Modernisierung des Datenschutzrechts würde unterstützt, wenn flankierend die informationelle Selbstbestimmung als Grundrecht der Informationsgesellschaft in das Grundgesetz aufgenommen würde.[185] Damit würde nicht ein neues Grundrecht geschaffen,[186] sondern die Konkretisierung der Grundrechte des Persönlichkeitsschutzes und der Menschenwürde sowie des Kommunikationsgehalts aller Grundrechte durch die ständige Rechtsprechung des Bun-

---

178 S. z.B. *Dammann/Simitis*, Art. 7 Rn. 2; entgegen dem eindeutigen Wortlaut a.A. *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 7 Rn. 6, 11; nach *Brühann*, Rn. 20, sind zwar Präzisierungen in der Form möglich, dass bestimmte Formen der Datenverarbeitung von einem verstärkten Widerspruchsrecht oder einer Einwilligung abhängig gemacht werden, doch könnten die Mitgliedstaaten nicht vom Begriff der „berechtigten" Interessen" abrücken (Rn. 21).

179 S. Teil 3 Kap. 3.1.4.

180 Erwägungsgrund 7 und 8.

181 Erwägungsgrund 9.

182 S. z.B. *Garstka*, DVBl. 1998, 986.

183 *Brühann*, in: *Grabitz/Hilf*, A 30, Art. 1 Rn. 12.

184 S. hierzu z.B. Teil 3 Kap. 3.1.4.

185 Ebenso z.B. *Schrader*, CR 1994, 427 ff.; *Kunig*, Jura 1993, 598; dagegen z.B. *Kloepfer* 1980, 49 ff.

186 Zur Geschichte der Bemühung um eine Aufnahme in das Grundgesetz s. z.B. *Kloepfer* 1998, 36 und 48.

desverfassungsgerichts auch durch den Verfassungsgesetzgeber explizit anerkannt. Dadurch würde gegenüber den Bürgern und den verantwortlichen Stellen ein rechtspolitisches Signal gesetzt und die besondere Bedeutung des Datenschutzes in der Entwicklung zur Informationsgesellschaft betont.

Das Grundrecht sollte allerdings nicht allein persönlichkeitsrechtlich gefasst, sondern als Kommunikationsgrundrecht ausgestaltet werden, das als Querschnittsgrundrecht den kommunikativen Gehalt aller Grundrechte zum Ausdruck bringt. Zusammen mit den anderen kommunikationsbezogenen Grundrechten muss es in der Lage sein, die verfassungsrechtliche Grundlage einer umfassenden Informations- und Kommunikationsordnung zu bieten.

Seine Aufnahme in den Grundrechtskatalog würde sowohl den abwehrrechtlichen, als auch den – in der Praxis häufig vernachlässigten – objektivrechtlichen Gehalt der informationellen Selbstbestimmung als Voraussetzung einer auf Freiheit und Selbstbestimmung basierenden Demokratie und Gesellschaft zur Entfaltung bringen. Vor allem könnte der objektivrechtliche Gehalt des Grundrechts auch die Datenverarbeitung im nicht öffentlichen Bereich strukturieren. Darüber hinaus wäre klarzustellen, dass dieses Grundrecht durch ein qualifiziertes Gesetz im überwiegenden öffentlichen oder privaten Interesse eingeschränkt werden kann.

Für einen eigenen Grundgesetzartikel spricht auch, dass in den normativen Ebenen sowohl über als auch unter dem Grundgesetz der Datenschutz ausdrücklich grundrechtlich verankert ist. Bereits zehn Landesverfassungen haben ein Datenschutzgrundrecht ausdrücklich in ihren Grundrechtskatalog aufgenommen[187] und auch Art. 8 der Europäischen Grundrechtecharta enthält ein – wenn auch nur unzureichend ausgestaltetes – Grundrecht auf Datenschutz.[188]

Die Modernisierung des Datenschutzrechts ist von der Anerkennung der informationellen Selbstbestimmung als Grundrecht in keiner Weise abhängig. Auch umgekehrt ist ihre Aufnahme ins Grundgesetz unabhängig von der Modernisierung des Datenschutzrechts zu empfehlen. Beide Vorhaben könnten sich jedoch gegenseitig unterstützen und befördern. Um Risiken im Gesetzgebungsprozess zu verringern, sollten sie allerdings formell als getrennte Gesetzgebungsvorhaben verfolgt werden.

[187] Berlin, Art. 33 der Verfassung von 1995, wörtliche Übernahme von Art. 21b aus dem Jahr 1990; Brandenburg, Art. 11 Abs. 1, 1992; Bremen, Art. 12 Abs. 4, eingefügt 1997; Mecklenburg-Vorpommern, Art. 6 Abs. 2, 1993; Nordrhein-Westfalen, Art. 4 von 1978, Rheinland-Pfalz, Art. 4a, eingefügt 2000; Saarland, Art. 2 Sätze 2 und 3 von 1985; Sachsen, Art. 33 von 1992; Sachsen-Anhalt, Art. 6 Abs. 1 Satz 2, 1992; Thüringen, Art. 6 Abs. 4, 1993; s. hierzu *Kunig*, Jura 1993, 597f.

[188] Das österreichische Datenschutzgesetz enthält in § 1 Abs. 5 einen Verfassungsartikel, der die unmittelbare Drittwirkung des Grundrechts auf Datenschutz vorsieht. Danach kann das Grundrecht gegen privatrechtliche Rechtsträger im ordentlichen Rechtsweg geltend gemacht werden.

Teil 3

Struktur und Inhalt eines künftigen Bundesdatenschutzgesetzes

1. Schutzgut: Informationelle Selbstbestimmung

Schutzgut des Datenschutzrechts ist die informationelle Selbstbestimmung, die in drei Ausprägungen zu berücksichtigen ist:

Die informationelle Selbstbestimmung hat ihren Kern im Schutz der Persönlichkeit und der Menschenwürde und wurde vom Bundesverfassungsgericht als risikoorientierte Ausprägung dieser Grundrechte in der Informationsgesellschaft entwickelt. Die informationelle Selbstbestimmung darf jedoch nicht auf das Persönlichkeitsrecht aus Art. 2 Abs. 1 GG reduziert werden. Sie gewinnt vielmehr ihre große Bedeutung dadurch, dass sie als Grundlage einer freien und demokratischen Kommunikationsverfassung ein aus allen Kommunikationsgrundrechten abzuleitendes Freiheitsrecht ist.[189] Das Recht auf informationelle Selbstbestimmung erstreckt sich auf alle personenbezogenen Daten und betrifft alle Formen ihrer Erhebung und Verwendung. Es ist nicht auf die automatische Datenverarbeitung, auf bestimmte Verarbeitungsphasen oder auf die Verwendung in Dateien beschränkt.[190]

Daneben wird die Bedeutung des in Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnisses in dem Maß zunehmen, in dem Telekommunikation zu einer beherrschenden Funktion der Informationsgesellschaft wird. Soweit durch den Kommunikationsvorgang personenbezogene Daten entstehen oder betroffen sind, ist das Telekommunikationsgeheimnis als eine bereichsspezifische Ausformung des Rechts auf informationelle Selbstbestimmung anzusehen, auf das das Bundesverfassungsgericht die Maßstäbe des Volkszählungsurteils anwendet.[191] Somit sind personenbezogene Daten außerhalb von Telekommunikationsvorgängen durch das Recht auf informationelle Selbstbestimmung, im Zusammenhang mit Telekommunikationsvorgängen durch dessen spezifische Ausprägung in Art. 10 Abs. 1 GG und als Inhalt von Telekommunikationsvorgängen durch das eigenständige Telekommunikationsgeheimnis geschützt.[192] Für eine Welt allgegenwärtiger Datenverarbeitung, die alle Lebensbereiche durchdringt, sollte das Grundrecht aus Art. 10 Abs. 1 GG dahin konkretisiert werden, dass es eine unbefangene und das heißt unbeobachtbare Kommunikation gewährleistet.[193]

Der Schutz der Selbstbestimmung durch beide Grundrechte wird ergänzt und verstärkt durch weitere Grundrechtsgarantien, die wegen des Inhalts und des Kontexts der Daten oder der Kommunikation oder im Hinblick auf die beeinträchtigenden Folgen ihrer Verwendung einschlägig sind.[194] Dies gilt zum Einen beispielsweise für soziale Näheverhältnisse, wie sie

---

189 S. auch *Gallwas*, Der Staat 18 (1979), 514; *Geis*, CR 1995, 171; *Hoffmann-Riem*, AöR 1998, 521.; *Simitis*, DuD 2000, 719; *Bizer*, DuD 2001, 274; *Trute*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5 Rn. 64; zu einem Datenschutzgrundrecht als Querschnittsgrundrecht s. auch *Kloepfer* 1980, 42 – s. aus der Rspr. des *BVerfG* z.B. *BVerfGE* 67, 100 (142f.); 77, 1 (46f.) hinsichtlich Art. 14 Abs. 1 GG und *BVerfG*, NJW 2001, 505 hinsichtlich der durch die allgemeine Handlungsfreiheit geschützten Freiheit im wirtschaftlichen Verkehr.

190 *BVerfGE* 84, 192 (195).

191 *BVerfGE* 85, 386 (395f.); 100, 313 (359).

192 S. z.B. *Groß*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 8.7.

193 S. hierzu auch die Erklärung der Datenschutzbeauftragten von Berlin, Brandenburg, Bremen, Nordrhein-Westfalen und Schleswig-Holstein vom 4.11.1998, DuD 1999, 69, Nr. 9; eine grundrechtliche Gewährleistung der Unbeobachtbarkeit sieht *Schulz*, Verwaltung 1999, 140.

194 *BVerfGE* 100, 313 (365).

durch Art. 6 GG geschützt sind,[195] für die Wohnung als privater Rückzugsbereich (Art. 13),[196] für innere Einstellungen (Art. 4 Abs. 1 GG), die negative Bekenntnisfreiheit (Art. 4 Abs. 2 GG),[197] die positiven und negativen Kommunikationsfreiheiten (Art. 5 Abs. 1 Satz 1 GG) sowie für die durch Art. 5 Abs. 3, Art. 8, Art. 12 GG geschützten Verhaltensfreiheiten.[198] Dies gilt zum Anderen vor allen Dingen für die in §§ 201 bis 206 StGB geschützten Geheimnisse, die weitgehend ihre Grundlage in verfassungsrechtlich geschützten Vertrauensverhältnissen haben, wie im Beichtgeheimnis (Art. 4 GG), im Vertrauensverhältnis zwischen Presse/Rundfunk und Informanten[199] sowie in der Vertraulichkeit der Redaktionsarbeit (Art. 5 Abs. 1 Satz 2 GG),[200] im Arzt-Patienten-Verhältnis oder im Rechtsanwalts-Mandanten-Verhältnis (Art. 12 GG).[201] Drittens sind die durch Art. 14 Abs.1 GG und Art. 2 Abs. 1 GG geschützten Geheimnisse bei wirtschaftlicher Betätigung als Grundlage der informationelle Selbstbestimmung zu berücksichtigen.[202] Die rechtlich geschützten Geheimnisse sind bei datenschutzeinschränkenden Regelungen (Ausnahmen im BDSG und in bereichsspezifischen Gesetzen) und deren Auslegung als Schranke der Einschränkung zu berücksichtigen. Ansonsten ist klarzustellen, dass ihr Schutzniveau durch allgemeine (sie nicht speziell erwähnende Regelungen) nicht berührt wird. Eine Integration von Geheimnisschutzregelungen ins BDSG – über das Datengeheimnis und die Straf- und Ordnungswidrigkeitenvorschrift in §§ 43 und 44 BDSG hinaus – könnte nach einer Abstimmung und Systematisierung des rechtlichen Geheimnisschutzes ein nächster Schritt der gesetzgeberischen Entwicklung sein.

Diese Grundrechte gemeinsam bilden die normative Grundlage für die rechtliche Gewährleistung individueller und kollektiver Freiheitsentfaltung in einer Gesellschaft, die von ubiquitärer Datenverarbeitung geprägt ist. Das Datenschutzgesetz dient dem Schutz dieser Grundrechte, ermöglicht aber auch im überwiegenden öffentlichen und privaten Interesse ihre Einschränkung.

2. Anwendungsbereich

Der Anwendungsbereich des Gesetzes sollte sich auf alle Formen der Verarbeitung personenbezogener Daten erstrecken.[203] Er sollte nicht durch die Unterscheidungen zwischen manueller und automatisierter Datenverarbeitung und zwischen Verarbeitung in Dateien, Akten oder sonstigen Formen geprägt sein. Zwar bezieht sich nach Art. 3 DSRL der Anwendungsbereich der Richtlinie allein auf Dateien und nicht auf Akten.[204] Diese unterschiedlichen Verarbeitungsformen beschreiben jedoch nicht die Grenze zwischen dem erforderlichen Schutz der Schutzgüter und irrelevanten Verhaltensweisen und führen zu unsachlichen Abgrenzungen.[205] Soweit dies zweckmäßig ist, sind bestimmte organisatorische oder technikbezogene Pflichten

---

195 S. z.B. *BVerfGE* 56, 363 (384); 57, 361 (382f.); 80, 81 (90 ff.); 101, 361 (386, 395).

196 S. z.B. *Burchard*, KritV 1999, 243.

197 S. z.B. *Albers* 1996, 137.

198 S. hierzu *Trute*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5.

199 *BVerfGE* 20, 162, 176 (187 ff.); 50, 234 (240); 77, 65 (74f.).

200 *BVerfGE* 66, 116 (130 ff.).

201 Sie werden ergänzt durch verfassungsrechtliche Garantien nicht grundrechtlicher Art, wie etwa durch das Zeugnisverweigerungsrecht nach Art. 47 GG.

202 S. zur Herleitung des Rechts auf informationelle Selbstbestimmung aus Art. 14 i.V.m. Art. 19 Abs. 3 GG *BVerfGE* 67, 100 (142f.); 77, 1 (46f.) sowie z.B.. *Schulze-Fielitz*, in: *Dreier*, GG, Art. 2 Rn. 67; *Hoffmann-Riem*, AöR 1998, 520; *Murswiek*, in: *Sachs*, GG, Art. 2 Rn 76.

203 *Simitis*, DuD 2000, 720: „Alle Verarbeitungen, gleichviel, ob sie off- oder online vorgenommen werden", sind „in einen von allgemeingültigen Grundsätzen geprägten und gestalteten Verarbeitungsrahmen einzufügen." S. auch S. *Bull*, RDV 1999, 149.

204 S. auch Erwägungsgrund 27.

205 Zumal durch Druck und Scannen jede Form der Datenverarbeitung mit geringem Aufwand immer auch in die andere Form überführt werden kann.

auf Dateien oder die automatisierte Datenverarbeitung zu beschränken. Auszunehmen vom Anwendungsbereich des Gesetzes ist nur die Datenverarbeitung zu ausschließlich persönlichen und familiären Zwecken und in einem diesen entsprechendem Umfang.

Das italienische Datenschutzgesetz[206] und das schweizerische Bundesgesetz über den Datenschutz[207] unterscheiden ebenfalls nicht zwischen unterschiedlichen Verarbeitungsformen. Art. 5 des italienischen Gesetzes schließt eine Unterscheidung zwischen manueller und automatisierter Datenverarbeitung sogar ausdrücklich aus. Das künftige allgemeine Datenschutzgesetz Japans unterscheidet zwischen „Basic Principles", die für jede Form der Datenverarbeitung gelten, und weitergehenden Verpflichtungen für verantwortliche Stellen, die geschäftsmäßig Dateien in Rechnern verarbeiten.[208] Auch nach den Safe Harbor Principles sind personenbezogene Daten in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person. Die Daten müssen nicht in einer Datei verarbeitet werden.[209]

2.1 Personenbezogene Daten

Die Regelungen des Datenschutzrechts beziehen sich auf personenbezogene Daten. Diese Begrenzung des Anwendungsbereichs sollte beibehalten werden. Der Begriff der personenbezogenen Daten, der auch die auf Personen beziehbare Daten erfasst, hat sich bewährt. Er ist ausreichend abstrakt, um auch neue Kategorien von Daten wie etwa biometrische und genetische Daten einzubeziehen,[210] und präzis genug, um in der Praxis zu ausreichend klaren Abgrenzungen zu führen. Hinsichtlich anonymer und pseudonymer Daten ist die Grenze der Personenbeziehbarkeit durch eine praktisch ausreichende Sicherheit (niedrige Wahrscheinlichkeit), einen Personenbezug herstellen zu können, zu bestimmen.[211]

In der Welt künftiger vernetzter und allgegenwärtiger Datenverarbeitung wird es immer öfter vorkommen, dass Daten – etwa zu Netzadressen oder zu anderen „Identifier" – verarbeitet werden, für die zu diesem Zeitpunkt unbekannt ist, ob sie sich auf bestimmte Personen beziehen (Beispiel: IP-Adressen), auf welche Personen sie sich beziehen (Beispiel: GUID) oder welchen Personen sie künftig zugeordnet werden (Beispiel: RFID-Tags). Auch wenn diese Daten zu diesem Zeitpunkt (noch) nicht den Begriff der personenbezogenen Daten erfüllen, sollten im Sinn der Vorsorge dennoch die Grundsätze der Vermeidung der Personenbezugs, der Erforderlichkeit und der Zweckbindung auf sie Anwendung finden, wenn zu erwarten ist, dass der Personenbezug hergestellt wird oder werden kann. Dürften diese Daten frei gesammelt, gespeichert, verbreitet oder veröffentlicht werden, könnte dies zu großen Benachteiligungen führen, wenn nachträglich der Personenbezug hergestellt und der Datensatz der Person zugeordnet werden könnte.[212]

2.2 Gewichtung personenbezogener Daten

Grundsätzlich gibt es keine harmlosen Daten. Im Volkszählungsurteil hat das Bundesverfassungsgericht kategorisch festgestellt:

---

206 Gesetz Nr. 675 vom 31.12.1996.

207 Gesetz vom 19.6.1992 (Stand. 7.7.1998).

208 Japanische Expertenkommission 2000.

209 S. Grundsätze des „sicheren Hafens" zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 11.

210 S. z.B. *Dix*, DuD 1989, 235; *Simitis* 1994, 107; *ders*., NJW 1998, 2477f.; *Burchard*, KritV 1999, 244; *Weichert*, DANA 2/2000, 7; s. auch *Simitis*, DuD 2000, 720; *Golembiewski*, NJW 2001, 1036. Das kanadische Datenschutzgesetzes erwähnt diese Daten ausdrücklich, s. *Huband*, DuD 2000, 461 ff.

211 S. zur Definition Teil 3 Kap. 3.4.3.

212 S. zum vergleichbaren Problem bei Pseudonymen Teil 3 Kap. 3.4.3.

„Unter den Bedingungen der automatischen Datenverarbeitung (gibt es) kein belangloses Datum. ... Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs.“[213]

Auch wenn es keine belanglosen Daten gibt,[214] so ist doch die Wahrscheinlichkeit ihrer unerwünschten Verwendung unterschiedlich groß.[215] Die Erkenntnis, dass bestimmte Daten typischerweise bestimmte soziale Folgen haben oder zumindest Gefährdungen der Beeinträchtigung mit sich bringen und andere typischerweise nicht, kann eine Grundlage dafür bilden, dass der Gesetzgeber auf diese unterschiedlichen Gefährdungslagen reagieren kann und gegebenenfalls reagieren muss.[216] Das Gesetz sollte daher nach beiden Seiten der unterschiedlichen Sensitivität von Daten und ihrer wahrscheinlichen Verwendung Rechnung tragen.

Einerseits sollte die Verarbeitung besonders schützenswerter Daten[217] von zusätzlichen Voraussetzungen abhängig gemacht werden.[218]

Andererseits sollte die Verarbeitung personenbezogener Daten in einem allgemeinen Erlaubnistatbestand grundsätzlich zugelassen werden,[219] wenn wegen der Offenkundigkeit der Daten (Beispiel: „Der Papst ist katholisch“) oder der Art der Verarbeitung schutzwürdige Interessen der betroffenen Person offensichtlich nicht beeinträchtigt werden.[220] Dies gilt – zur Vermeidung absurder Ergebnisse – auch für besonders schützenswerte Daten.[221]

Wegen der von Art. 5 Abs. 1 Satz 1 GG gewährleisteten Informationsfreiheit ist ebenso die Erhebung und Speicherung personenbezogener Daten aus allgemein zugänglichen Quellen ohne Einschränkung zuzulassen. Ob diese Daten dann weiterverarbeitet und verwendet werden dürfen, richtet sich nach den allgemeinen Grundsätzen. Denn das Grundrecht aus Art. 5 Abs. 1 Satz 1 GG erfasst in seinem Schutzbereich nur die „Unterrichtung aus allgemein zugänglichen Quellen“ und schützt damit den Rezeptionsvorgang, also die Wahrnehmung der Informationen.[222] Da aber nicht nur eine Unterrichtung für den Augenblick garantiert ist, son-

---

213 *BVerfGE* 65, 1 (45).

214 S. hierzu näher *Simitis*, Revisiting Sensitive Data, http://www.coe.fr/dataprotection/eReport%20Simitis; *ders*. 1990, 469 ff.

215 S. hierzu auch *Hoffmann-Riem*, AöR 1998, 528 ff.

216 Dies ist nicht mit einer Rückkehr zur Sphärenlehre verbunden, sondern durchaus mit einer konstruktivistischen Perspektive vereinbar, die in typischen Verwendungen und den daraus für die Beteiligten entstehenden Folgen einen Grund für besondere Schutzbedürfnisse sieht - s. *Trute*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5 Rn. 29.

217 S. z.B. Art. 8 DSRL.

218 S. hierzu Teil 3 Kap. 3.1.5.

219 Dies bedeutet nicht eine Relativierung des Begriffs des Eingriffs in die informationelle Selbstbestimmung – s. hierzu Teil 2 Kap. 4.1, sondern dessen Bestätigung, da hier ein allgemeiner Erlaubnistatbestand für Eingriffe unterhalb einer bestimmten Sensitivitätsschwelle empfohlen wird. Weitergehender *Hoffmann-Riem*, AöR 1998, 531, der bloße Betroffenheiten nicht als Eingriffe in den Schutzbereich der informationellen Selbstbestimmung qualifizieren möchte.

220 S. z.B. § 6 Abs. 1 Satz 2 BlnDSG. Weil die Erhebung Teil der Datenverarbeitung ist, ergibt sich das Problem vorwiegend im Bereich sog. „trivialer Kommunikation“. Diese definierte der BfD, DVBl 1984, 614, als Weitergabe von Informationen, die weder ihrer Art nach noch aus dem Verwendungszusammenhang Schutzwürdigkeit beanspruchen können. S. hierzu mit Beispielen auch *Petersen* 2000, 130 ff.

221 Ein Beispiel dürfte etwa die Datenverarbeitung im Rahmen einer vom Bankkunden veranlassten Überweisung von Gewerkschaftsbeiträgen, Mitgliedschaftsbeiträgen an politische Parteien oder Spenden an weltanschauliche Vereinigungen sein. Die Übermittlung des Verwendungszwecks wird von § 676a Abs.1 BGB gefordert. Da der Überweisung weder eine spezifische Einwilligung nach § 4a Abs. 3 BDSG zugrunde liegt und auch keiner der Erlaubnistatbestände des § 28 Abs. 6 bis 9 BDSG die Datenverarbeitung rechtfertigt, könnte ohne eine Regelung wie sie hier vorgeschlagen wird, die Überweisung nicht ausgeführt werden.

222 S. *Degenhart*, in: BK-GG, Art. 5 Rn. 348.

dern die Informationsfreiheit Grundlage für die freie Meinungsbildung ist, gehört zum Tatbestandsmerkmal des Sich-Unterrichtens auch das Speichern von Informationen.[223] Weitere Verarbeitungsschritte oder Verwendungsweisen sind vom Schutzbereich der Informationsfreiheit allerdings nicht gedeckt, vielmehr ist zwischen der Informationsfreiheit einerseits und der späteren Verwendung bereits publizierter Angaben andererseits zu unterscheiden.[224] Schon das Zitieren aus allgemein zugänglichen Quellen, um andere zu unterrichten, fällt nicht mehr unter die Informationsfreiheit. Auch für Daten aus allgemein zugänglichen Quellen besteht das allgemeine datenschutzrechtliche Risiko, dass sie verfälscht, aus ihrem ursprünglichen Kontext herausgelöst und in neue Verwendungszusammenhänge eingefügt werden. Sobald sie der allgemein zugänglichen Quelle entnommen sind, werden diese Daten zu einer eigenständigen Informationsgrundlage, für deren Verarbeitung keine Privilegierung geboten ist.[225]

2.3 Verantwortliche Stelle

In einer vernetzten Welt allgegenwärtiger Datenverarbeitung wird Datenverarbeitung in vielfältigsten Formen mit unterschiedlichsten Beteiligten erfolgen. Für sie ist es nahezu ausgeschlossen, für alle relevanten Fälle den jeweils richtigen Adressaten der rechtlichen Regelung durch technische oder organisatorische Funktionsbeschreibungen zu benennen.

Zu recht stellt daher Art. 2 d) Satz 1 DSRL unmittelbar auf die Verantwortung einer jeden Stelle ab, indem sie den Begriff des „für die Verarbeitung Verantwortlichen" definiert als „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet". In Anpassung an diese Terminologie wurde in § 3 Abs. 7 BDSG die alte Definition der speichernden Stelle durch die der verantwortlichen Stelle ersetzt. Allerdings wurde gegenüber der DSRL der Kreis der Adressaten eingeengt, indem auf typische Verarbeitungshandlungen abgestellt wird. Verantwortliche Stelle ist danach, wer personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Bei dieser Definition besteht die Gefahr, dass durch sie nicht alle relevanten Teilschritte vernetzter, arbeitsteiliger von vielen unterschiedlichen Stellen mit unterschiedlichen Aufgaben durchgeführter Verarbeitungsprozesse (Netzwerke, Mobilkommunikation, mobile Agenten, Ubiquitous Computing) erfasst werden.

Daher sollte unmittelbar an der Definition der DSRL angeknüpft werden und als verantwortliche Stelle derjenige definiert werden, der allein oder mit anderen über Zwecke und Mittel der Datenverarbeitung *entscheidet*. Dies wird in der Regel derjenige sein, der in § 3 Abs. 7 BDSG definiert ist. Doch ist die hier vorgeschlagene Definition weitergehend und vermeidet Regelungslücken. Sie stellt auch sicher, dass in dem Fall, in dem für einzelne Abschnitte eines einheitlichen Datenverarbeitungskomplexes unterschiedliche Stellen über die Zwecke und Mittel der Verarbeitung zu entscheiden haben, diese nebeneinander als Verantwortliche der Verarbeitung anzusehen sind. Die Anforderungen an die Datenverarbeitung sind grundsätzlich von jeder verantwortlichen Stelle zu erfüllen. Sie können untereinander vereinbaren, dass im Innenverhältnis nur einer von ihnen bestimmte Datenschutzpflichten (wie z.B. Benachrichtigung oder Datenschutzerklärung) übernimmt, ohne sich dadurch gegenüber der betroffenen Person von den Verpflichtungen zu befreien.[226]

---

[223] So *Starck*, in: *v. Mangoldt/Klein/Starck*, GG Art. 5 Abs. 1, 2 Rn. 50; *Schulze-Fielitz*, in: *Dreier*, GG Art. 5 Rn. 63.

[224] s. *Simitis*, in: *ders. u.a.*, BDSG, § 28 Rn. 169.

[225] Der Erstellung von Profilen etwa durch Auswertung von Medienarchiven wäre damit die Grundlage entzogen.

[226] Zum Problem des Outsourcing s. Teil 3 Kap. 3.5.6.

Künftig wird die Bedeutung von „Intermediären“ zunehmen. Unter diesen können Stellen verstanden werden, die in die Kommunikation betroffener Personen eingeschaltet werden oder sonstige Leistungen für diese erbringen und dabei für die betroffene Person Daten verarbeiten. Beispiele sind – über die Telekommunikationsdiensteanbieter oder Internetprovider hinaus – Anbieter, von denen bei Bedarf Programme aus dem Netz abgerufen werden können, die für die betroffene Person Daten speichern oder archivieren, die Dienste von Softwareagenten anbieten oder die für die betroffene Person Datenschutzfunktionen im Internet wahrnehmen („Infomediaries“[227]). Gemeinsam ist diesen Beispielen, dass die genannten Stellen nicht nur Daten über die betroffene Person im Rahmen ihres Vertragsverhältnisses mit dieser („Bestandsdaten“) sowie zur Erbringung der Vertragsleistung („Nutzungsdaten“) verarbeiten, sondern auch viele weitere Daten der betroffenen Person („Inhaltsdaten“), die ihnen nur anvertraut sind. In dieser Hinsicht sind sie quasi als Treuhänder zwischengeschaltet oder eingesetzt. Diese Vertrauensstellung ist mit besonderen Pflichten und besonderen Risiken verbunden. Sie könnten die anvertrauten Daten für andere Zwecke verwenden, etwa für sich auswerten, weitergeben oder die aus ihnen erstellten Profile verkaufen. Die Daten könnten, auch wenn sie bei der betroffenen Person geschützt wären, bei den „Intermediären“ von Dritten leichter zur Kenntnis genommen werden.[228]

Trotz dieser besonderen Risiken wird hier vorerst nicht empfohlen, wie in der Begleitkommission angeregt worden war, für „Intermediäre“ neben verantwortlichen Stellen und betroffenen Personen eine eigene rechtliche Kategorie von Regelungsadressaten zu schaffen. Da „Intermediäre“ personenbezogene Daten verarbeiten, sind sie verantwortliche Stellen und unterliegen den im Folgenden beschriebenen Anforderungen an die Datenverarbeitung, müssen das Datengeheimnis wahren, die organisatorischen Anforderungen in Kap. 4 erfüllen und die in Kap. 7 dargestellten Rechte der betroffenen Personen beachten. Diese gesetzlichen Regelungen erscheinen ausreichend, um den genannten Risiken zu begegnen. Spezifische gesetzliche Regelungen für „Intermediäre“ erscheinen nicht erforderlich. Solche spezifischen Regelungen könnten durch selbstgesetzte Verhaltensregeln geschaffen werden.[229] Im Übrigen sind weitere rechtliche Ausgestaltungen dem vertraglichen Verhältnis zwischen „Intermediären“ und betroffenen Personen zu überlassen.[230] Dennoch sollte die Entwicklung von „Intermediären“ beobachtet und deren Regelungsbedarf von Zeit zu Zeit bewertet werden. Sollte das hier empfohlene Konzept zur gesetzlichen Regelung des Datenschutzes im Gesetzgebungsprozess nachhaltig verändert werden, muss geprüft werden, ob unter dem veränderten Regelungsrahmen für „Intermediäre“ eigenständige Regelungen erforderlich sind.

2.4 Schutz natürlicher und juristischer Personen

Bisher ist das Datenschutzrecht auf den Schutz der Persönlichkeitsrechte natürlicher Personen beschränkt. Personenvereinigungen und juristische Personen sind aus seinem Schutzbereich ausgeschlossen. Dies erscheint gerechtfertigt, soweit das Datenschutzrecht auf seinen ethisch-philosophischen Ausgangspunkt als Schutz der Persönlichkeit und Menschenwürde des Individuums beschränkt wird. Juristische Personen benötigen keinen rechtlichen Schutz für die Ausbildung und Entfaltung einer individuellen Persönlichkeit. Wenn der Begriff der personenbezogenen Daten aber weit über den Bereich des – menschenwürdebezogenen – Personengeheimnisses hinaus ausgedehnt wird und auch Wirtschaftsdaten (Erwerbs- und

[227] S. zu diesen z.B. *Grimm/Roßnagel*, DuD 2000, 450 m.w.N.

[228] Soweit diese sich nicht auf Schutzrechte der betroffenen Personen berufen können.

[229] S. Teil 3 Kap. 6.

[230] S. Teil 3 Kap. 3.1 und 3.3.

Konsumverhalten, Einkommen, Vermögen und weitere wirtschaftliche Angaben) umfasst, erscheint die Ungleichbehandlung zu juristischen Personen problematisch.[231]

Allerdings sprechen Gründe dafür, juristische Personen und rechtsfähige Personenvereinigungen in den Schutz eines modernen Datenschutzrechts aufzunehmen. Zum Einen gilt das Grundrecht auf informationelle Selbstbestimmung, soweit nicht gerade sein persönlichkeitsrechtlicher Kern betroffenen ist, nach Art. 19 Abs. 3 GG auch für juristische Personen.[232] Das Bundesverfassungsgericht erkennt ihnen unter ausdrücklicher Bezugnahme auf das Volkszählungsurteil einen „Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf sie bezogenen individualisierten oder individualisierbaren Daten“ zu.[233] Dabei kann offenbleiben, ob dieser Schutz aus Art. 2 Abs. 1 GG,[234] aus Art. 9 Abs. 1 GG[235] oder aus Art. 14 Abs. 1 GG[236] hergeleitet wird.[237] Wenn das Schutzgut des Datenschutzgesetzes das Grundrecht auf informationelle Selbstbestimmung ist,[238] dann sollte der Schutz des Gesetzes mit dem Schutz des Grundrechts deckungsgleich sein.[239]

Schutzgut des Gesetzes soll weiterhin das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG sein. Auch dieses gilt nach Art. 19 Abs. 3 GG für juristische Personen. Im Telekommunikationsdatenschutzrecht wird daher auch konsequent der Schutz nach § 89 Abs. 1 Satz 4 TKG und § 1 Abs. 1 Satz 2 TDSV auf juristische Personen erstreckt. Wenn künftig Telekommunikation ein Regelbestandteil der Datenverarbeitung wird und das Telekommunikations-Datenschutzrecht in das BDSG integriert werden soll, können dessen Regelungen weder auf natürliche Personen beschränkt werden noch den personellen Schutzbereich für Datenverarbeitung in und außerhalb der Telekommunikation unterschiedlich bestimmen.

Weiterhin ist zu berücksichtigen, dass das Datenschutzrecht auch außerhalb der Telekommunikation den Schutzbereich bisher schon nicht durchgängig auf natürliche Personen begrenzt hat. So bestimmt zum Beispiel § 35 Abs. 4 SGB I, dass Betriebs- und Geschäftsgeheimnisse personenbezogenen Daten gleich stehen. Das allgemeine Steuergeheimnis nach § 30 AO wie auch das Bankgeheimnis nach § 30a AO gelten heute als Grundrechtsgewährleistung der in-

---

231 S. z.B. *Kloepfer* 1980, 12, 26; *ders*. 1998, 50 und 82f.; s. auch *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1 Rn. 5.

232 S. zur Diskussion z.B. *Kunig*, Jura 1993, 599.

233 *BVerfGE* 67, 100 (142f.); 77, 1 (46f.). Im Gegensatz zu diesen beiden Entscheidungen des Zweiten Senats hat die 1. Kammer des Ersten Senats es neuerdings ausdrücklich offengelassen, ob und inwieweit juristische Personen sich „in Fällen wie dem vorliegenden“ (Auskunft über Kundenkonten an Finanzamt) auf das Grundrecht auf informationelle Selbstbestimmung berufen können – *BVerfG*, NJW 2001, 811 – und ob ihr Schutz gegen Preisgabe von Grundbucheinträgen auf das Recht auf informationelle Selbstbestimmung oder auf die durch die allgemeine Handlungsfreiheit geschützte Freiheit im wirtschaftlichen Verkehr gestützt wird – *BVerfG*, NJW 2001, 505.

234 Die 1. Kammer des Ersten Senats hat den Schutz juristischer Personen gegen die Preisgabe von individualisierten Daten auch auf die durch die allgemeine Handlungsfreiheit geschützte Freiheit im wirtschaftlichen Verkehr gestützt– *BVerfG*, NJW 2001, 505.

235 S. *Kunig*, Jura 1993, 599 für Vereinigungen; ebenso *Schulze-Fielitz*, in: *Dreier*, GG, Art. 2 Rn. 67.

236 Das *BVerfG* leitet den „grundrechtlichen Datenschutz“ auch aus Art. 14 Abs. 1 GG her – s. *BVerfGE* 67, 100 (142f.); 77, 1 (46f.). Zur Herleitung eines Rechts auf informationelle Selbstbestimmung aus Art. 14 i.V.m. Art. 19 Abs. 3 GG s. z.B.. *Schulze-Fielitz*, in: *Dreier*, GG, Art. 2 Rn. 67; *Hoffmann-Riem*, AöR 1998, 520; *Murswiek*, in: *Sachs*, GG, Art. 2 Rn 76.

237 Zum Grundrecht auf informationelle Selbstbestimmung als Ausdruck des kommunikativen Gehalts aller in Frage kommenden Grundrechte s. Teil 3 Kap. 1.

238 S. Teil 3 Kap. 1.

239 Dies gilt auch, wenn der grundrechtliche „Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf sie bezogenen individualisierten oder individualisierbaren Daten“, *BVerfGE* 67, 100 (142f.); 77, 1 (46f.), nicht aus der informationelle Selbstbestimmung, sondern aus dem auf Art. 12 und 14 GG zurückführbaren Schutz wirtschaftlicher Geheimnisse begründet wird – s. zu Geheimnissen als Schutzgegenstand des Datenschutzrechts Teil 3 Kap. 1.

formationellen Selbstbestimmung[240] und erstrecken sich gleichermaßen auf natürliche und juristische Personen.

Schließlich ist die Abgrenzung zwischen Daten natürlicher und juristischer Personen in der Aufsichtstätigkeit ohnehin häufig schwierig oder unmöglich. Dateien über juristische Personen enthalten in der Regel auch Daten zu natürlichen Personen. Vielfach kann einem Datum – etwa im Bereich der Telekommunikation – zum Zeitpunkt einer Entscheidung über den notwendigen Schutz nicht angesehen werden, ob es einer natürlichen oder einer juristischen Person zuzuordnen ist. Dies wird in der künftigen Welt allgegenwärtiger Datenverarbeitung noch viel weniger möglich sein. Daher werden die Daten in der Praxis grundsätzlich ohne weitere Differenzierung dem höheren Schutzniveau unterstellt. Vieles spricht dafür, die in der Praxis ohnehin irrelevante Unterscheidung aufzugeben. Die Einbeziehung juristischer Personen wäre somit auch praxisadäquat.

Zwar hat es aufgrund dieser Praxis und der direkten Anwendung der informationellen Selbstbestimmung auf juristische Personen bisher keinen drängenden Bedarf gegeben, das Datenschutzgesetz auf sie zu erstrecken. Auch bieten die Regelungen zu Betriebs- und Geschäftsgeheimnissen und zur Verhinderung unlauteren Wettbewerbs einen gewissen Schutz. Diese Regelungen und die geltende Praxis verringern den rechtspolitischen Druck auf eine Einbeziehung juristischer Personen, auch wenn sie nur Wettbewerbsunternehmen und nicht andere Gesellschaften und Vereinigungen schützen.

Die Erfahrungen mit diesen Regelungen reduzieren aber zugleich auch die in der Begleitkommission und in den Fachgesprächen von manchen befürchteten Risiken eines solchen Schritts. Rechtsfolgen des Einbezugs juristischer Personen wären vor allem, dass sie an den Transparenzgeboten (Benachrichtigung, Erhebung bei der betroffenen Person) beteiligt werden und dass die Verarbeitung von Daten über sie, die nicht offenkundig sind oder veröffentlicht werden müssen, einer Rechtfertigung bedarf.[241] Die juristischen Personen könnten Auskunfts-, Berichtigungs- und Löschungsrechte geltend machen. In der Praxis wird der Einbezug juristischer Personen des Privatrechts keine gravierenden Folgen haben. Sie haben im Telekommunikations-Datenschutzrecht seit langem Schutz- und Kontrollrechte. Dort werden sie durch die Erlaubnistatbestände und die Einschränkungen und Bedingungen der Datenverarbeitung geschützt. Sie können nach § 89 TKG und der TDSV die Rechte auf Unterrichtung (über die Datenverarbeitung, die Einwilligung und das Widerspruchsrecht) und auf Abrufen des Inhalts der Einwilligung sowie über § 1 Abs. 2 TDSV die im BDSG vorgesehenen Transparenzgebote und Betroffenenrechte geltend machen. Dieser Schutz und diese Rechte juristischer Personen haben seit ihrem Bestehen zu keinerlei negativen Folgen für den Datenschutz geführt.

Daher sprechen die gewichtigeren Argumente dafür, die Modernisierung des Datenschutzrechts auch zu einer Vereinheitlichung und Harmonisierung der Regelungen zum geschützten Personenkreis zu nutzen. Das Datenschutzrecht entwickelt sich immer weiter vom Persönlichkeitsschutz ausgehend hin zu einem Verkehrsrecht des Informationszeitalters, in dem künftig vor allem Maschinen mit Maschinen kommunizieren, von denen man nicht weiß, wer hinter ihnen steht. Bezugspunkte sind dann nur noch abstrakte Entitäten, für die eine Differenzierung nach Rechten nicht mehr sinnvoll ist.

Bei einer Erstreckung des Datenschutzes auf juristische Personen kann allerdings der materielle Unterschied zwischen juristischen und natürlichen Personen nicht ganz vernachlässigt werden. Soweit Regelungen ausdrücklich dem Schutz der Privatsphäre oder dem Persönlich-

---

[240] *Kruse*, Lehrbuch des Steuerrechts I, München 1991, 344f.

[241] Dies schränkt Presseberichte über juristische Personen in keiner Weise ein – s. selbst zu Presseberichten über natürliche Personen *BVerfGE* 99, 185 (194 ff.); 101, 361 (380 ff.); *BVerfG*, AfP 2000, 450f.

keitsrecht dienen (z.B. Schutz sensitiver Daten, Schutz vor Profilen, Schadensersatz für schwere Verletzungen des Persönlichkeitsrechts), können sie nur auf natürliche Personen Anwendung finden. Auch sollte das Recht, anonym oder pseudonym handeln zu können, auf natürliche Personen beschränkt werden. Im Gegenteil sollte ausdrücklich klargestellt werden, dass Publizitäts-, Unterrichtungs-, Auskunfts- und sonstige Informationspflichten von juristischen Personen und rechtsfähigen Personenvereinigungen in anderen Rechtsvorschriften durch das Datenschutzrecht in keiner Weise berührt werden.

Für einen denkbaren Konflikt zwischen verantwortlicher Stelle und betroffener Person ist klarzustellen, dass die verantwortliche Stelle sich gegenüber einer betroffenen Person, die Betroffenenrechte geltend macht, nicht selbst auf Betroffenenrechte berufen kann. Betriebs- und Geschäftsgeheimnisse oder Berufsgeheimnisse bleiben – wie bisher – unberührt.

Die europäische Datenschutzrichtlinie steht einer Aufnahme der juristischen Personen in den Kreis der vom BDSG Geschützten nicht entgegen. In Erwägungsgrund 24 wird ausdrücklich darauf hingewiesen, dass die Richtlinie „nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen", berührt. Die Richtline schützt juristische Personen nicht, stellt sich einem Schutz aber auch nicht entgegen. Ein Schutz juristischer Personen steht somit in keinem Widerspruch zur Richtlinie, soweit dadurch die durch die Richtlinie geschützten Rechte betroffener natürlicher Personen nicht eingeschränkt werden.

Die Aufnahme juristischer Personen in den Kreis der vom Datenschutzrecht geschützten Personen wird empfohlen, zugleich aber festgestellt, dass alle anderen Vorschläge zur einer Modernisierung des Datenschutzrechts nicht von der Umsetzung dieses Vorschlags abhängig sind.

Juristische Personen werden auch durch Art. 3 b) des Schweizerischen Bundesgesetzes über den Datenschutz[242] ebenso wie durch § 4 Nr. 3 des Österreichischen Bundesgesetzes über den Schutz personenbezogener Daten[243] in gleicher Weise als betroffene Personen angesehen wie natürliche Personen. Das italienische Datenschutzgesetz[244] schützt nach Art. 1 auch juristische Personen und jede andere Gesellschaft oder Vereinigung. Nach der Definition in Art. 1 Abs. 2 c) sind personenbezogene Daten auch Daten von juristischen Personen und jeder anderen Gesellschaft oder Vereinigung.

2.5 Datenverarbeitung

Jeder Umgang mit personenbezogenen Daten sollte unter einer *einheitlichen Bezeichnung* erfasst werden. Die informationelle Selbstbestimmung ist nur dann gewahrt, wenn das Recht des Einzelnen, selbst über die Preisgabe und Verwendung der die eigene Person betreffenden Daten zu entscheiden, sowohl beim ersten Zugriff als auch bei jeder späteren Benutzung beachtet wird. Die Erhebung ist keine minder bedeutsame Vorbereitungshandlung, vielmehr ist ein „Eingriff" in das Grundrecht „schon die Erfassung selbst".[245]

Für diesen umfassenden Begriff bietet sich die Bezeichnung der „Datenverarbeitung" an, weil diese der Definition des Art. 2 b) DSRL entspricht und auch in den meisten europäischen Datenschutzgesetzen Verwendung findet. Diese Bezeichnung umschreibt jeden Umgang mit personenbezogenen Daten und sollte als Beispiele die Begriffe „Erheben, Speichern, Anpassen, Verändern, Aggregieren, Re-Identifizieren, Auslesen, Abfragen, Übermitteln, Verbreiten,

---

[242] Gesetz vom 19.6.1992 (Stand. 7.7.1998); s. auch Art. 2 der den Schutz ausdrücklich auch auf juristische Personen erstreckt.

[243] Datenschutzgesetz 2000, BGBl. I Nr. 165/1999.

[244] Gesetz Nr. 675 vom 31.12.1996.

[245] *BVerfGE* 100, 313 (366).

Bereitstellen und Nutzen“ aufführen. Grundsätzlich wird zur Bezeichnung der regulierten Tätigkeit nur der alle Phasen umfassende Begriff der „Datenverarbeitung“ verwendet. Nur dort, wo es tatsächlich notwendig ist, sollte im Gesetz auf besondere Formen der Datenverarbeitung eingegangen werden. Nur in diesem Fall ist die Definition einer Unterform der Datenverarbeitung notwendig. Ein einheitlicher Verarbeitungsbegriff vermeidet Schutzlücken, entlastet den Gesetzestext und schafft Klarheit für alle Anwender.

Nach dem informellen Entwurf eines Arbeitnehmerdatenschutzgesetzes aus dem Bundesministerium für Arbeit- und Sozialordnung soll in Umsetzung der DSRL Verarbeitung definiert werden als jeder mit oder ohne Hilfe automatisierter Verfahren durchgeführte Vorgang oder jede Vorgangsreihe in Zusammenhang mit personenbezogenen Daten der Arbeitnehmer wie das Erheben, Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.[246]

Nach § 2 Abs. 2 DSG SH ist ebenfalls Datenverarbeitung der übergeordnete Begriff, der mit der „Verwendung“ personenbezogener Daten gleichgesetzt wird. Der Entwurf für ein BDSG von Bündnis90/Die Grünen geht vom „Umgang“ als übergeordneter Kategorie aus.

Das italienische Datenschutzgesetz[247] sieht in Art. 1 Abs. 2 b) auch einen einheitlichen Begriff der Datenverarbeitung vor, der alle Operationen mit personenbezogenen Daten umfasst, unabhängig davon, ob diese mit elektronischen oder automatischen Mitteln verarbeitet werden. Ebenso enthält das Niederländische Datenschutzgesetz[248] in Art. 1 b) einen einheitlichen Begriff der Datenverarbeitung. Allerdings wird der Anwendungsbereich des Gesetzes in Art. 2 Abs. 1 auf die vollständige oder teilweise automatisierte Datenverarbeitung und die nichtautomatisierte Verarbeitung in einer Datei oder für eine Datei beschränkt. Einen einheitlichen und alle Formen erfassenden Begriff der Datenverarbeitung verwenden ebenfalls § 4 Nr. 8 des Österreichischen Bundesgesetzes über den Schutz personenbezogener Daten,[249] Art. 3 b) des portugiesischen Datenschutzgesetzes,[250] Section 3 (2) des finnischen Datenschutzgesetzes,[251] Section 1 (1) des britischen Data Protection Acts 1998[252] und Section 3 des schwedischen Datenschutzgesetzes.[253] Nach dem künftigen allgemeinen Datenschutzgesetz Japans soll „processing“ „any operation concerning personal information and including its use“ umfassen.[254]

2.6 Verarbeitung ohne gezielten Personenbezug

In einer Zukunft, in der viele Alltagsgegenstände untereinander Daten austauschen, fast alle Datenverarbeitungsprozesse über Netze auf Daten, Programme und Ressourcen zugreifen und bald jede Handlung im Netz und außerhalb Datenspuren hinterlässt,[255] macht es wenig Sinn, alle diese Formen der Datenverarbeitung einheitlichen Anforderungen zu unterwerfen. Da außerdem das Multimedia- und Telekommunikations-Datenschutzrecht ins BDSG integriert werden soll, ist zwischen den beiden folgenden Kategorien der Datenverarbeitung

---

246 S. dazu *Tinnefeld/Viethen*, NZA 2000, 981.

247 Gesetz Nr. 675 vom 31.12.1996.

248 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

249 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999.

250 Gesetz Nr. 67/98 zum Schutz personenbezogener Daten vom 26.10.1998.

251 Datenschutzgesetz (523/1999) vom 22.4.1999.

252 Data Protection Act vom 18.7.1998.

253 Datenschutzgesetz (1998:204) vom 29.4.1998.

254 Japanische Expertenkommission 2000, 4.

255 S. Teil 1 Kap. 2.1.

- *Verarbeitung mit gezieltem Personenbezug* zum Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Personalakten, Vertragsdaten, Bestandsdaten) und
- *Verarbeitung ohne gezielten Personenbezug* zu anderen Zwecken als dem Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Erbringen technischer Dienstleistungen, Kommunikation von Maschine zu Maschine, „Überschussdaten" bei Suchprozessen)

zu unterscheiden. Für sie sollten unterschiedliche Anforderungen gestellt werden. Während für die Verarbeitung mit gezieltem Personenbezug die im folgenden dargestellten Verarbeitungsregeln gelten, sollten diese Anforderungen für die Verarbeitung ohne gezielten Personenbezug risikoadäquat und effizienzsteigernd spezifiziert werden. Da es dem Datenverarbeiter nicht auf die Verarbeitung der Daten ankommt, sollte er verpflichtet werden, sie auf das erforderliche Minimum zu begrenzen, während ihrer Verarbeitung gegen Zweckentfremdung zu schützen und nach der Verarbeitung sofort zu löschen. Die Daten sollten einer strengen Zweckbindung (wie nach § 31 BDSG) unterliegen und vor einer Zweckänderung durch ein Verwertungsverbot geschützt sein.[256] Zur Unterstützung der Zweckbindung sollte ein Verstoß gegen sie in die Bußgeldvorschrift des § 43 BDSG aufgenommen werden. Soweit die verantwortliche Stelle sicherstellt, dass diese Daten nicht in die Form gezielter Datenverarbeitung überführt werden, sollte sie in einem allgemeinen Erlaubnistatbestand zugelassen werden. Ein Anspruch auf Auskunft über einzelne Daten erscheint eher kontraproduktiv. Die Daten und die Orte ihrer Verarbeitung sind dem Verarbeiter in der Regel selbst nicht bekannt und für ihn auch uninteressant. Ein Auskunftsanspruch hätte hier den unerwünschten Effekt, dass er Protokollverfahren oder Data-Mining-Techniken nur deshalb anwenden müsste, um die personenbezogenen Daten ausfindig zu machen und zusammenzuführen.[257] Statt dessen sollte er die Zwecke und die Struktur der Datenverarbeitung in einer Datenschutzerklärung allgemein darstellen.[258]

Eine Regelung der Datenverarbeitung ohne gezielten Personenbezug könnte etwa folgende Grundstruktur aufweisen:

Personenbezogene Daten, die ausschließlich zu dem Zweck verarbeitet werden, kurzfristig

1. *Telekommunikations- und Teledienste,*
2. *Kommunikation zwischen automatisch tätigen Maschinen oder*
3. *Verfahren zur Suche nach personenbezogenen Daten*

technisch zu ermöglichen und unmittelbar nach Erfüllung dieses Zwecks gelöscht werden, dürfen verarbeitet werden, wenn die verantwortliche Stelle

1. *in ihrer Datenschutzerklärung diese Voraussetzungen nachgewiesen,*
2. *so wenig personenbezogene Daten wie möglich verarbeitet und*
3. *die Verarbeitung der personenbezogenen Daten zu anderen Zwecken durch Sicherungsmaßnahmen ausgeschlossen hat.*

In diesem Regelungsvorschlag wird der Begriff der Datenverarbeitung ohne gezielten Personenbezug nicht als gesetzliches Tatbestandsmerkmal verwendet. Er dient nur als neue dogmatische Kategorie, um für unterschiedliche Tatbestände das entscheidende gemeinsame Merkmal zum Ausdruck zu bringen. Um eine ausreichende Rechtssicherheit zu erreichen,

---

256 S. Teil 3 Kap. 3.5.3

257 Zur europarechtlichen Zulässigkeit, den individuellen Auskunftsanspruch durch eine generelle Auskunft über die Struktur der Datenverarbeitung zu ersetzen – s. Teil 3 Kap. 7.1.2.

258 S. hierzu Teil Kap. 7.1.2.

enthält der Regelungsvorschlag für die Bestimmung seines Anwendungsbereichs drei Fallgruppen, auf die die Regelung begrenzt ist. Damit wird auch dem Petitum der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Rechnung getragen.[259]

Die Unterscheidung der Datenverarbeitung mit gezieltem und ohne gezielten Personenbezug ist für das deutsche Datenschutzrecht nicht vollkommen neu. Sie findet zum Beispiel Anwendung, um das datenschutzrelevante Erheben von Daten von deren nicht relevantem Erfassen zu unterscheiden. So stellt das Bundesverfassungsgericht in der Entscheidung zu den Abhörmöglichkeiten des BND fest:

> „An einem Eingriff fehlt es ..., soweit Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden."[260]

In ähnlicher Weise sieht das *OLG Bremen*[261] keine Erhebung, wenn der Konkursverwalter zufällig Patientendaten beim Öffnen der Post des Gemeinschuldners zur Kenntnis nimmt. Nach der bisherigen Dogmatik setzt die Erhebung ein aktives, zielgerichtetes Verhalten der verantwortlichen Stelle voraus, das grundsätzlich auf die weitere Nutzung der erhobenen Daten abzielt.[262] Lediglich bei Gelegenheit anderer Tätigkeiten erfolgende Kenntnisnahmen, die eher zwangsläufig oder zufällig erfolgen, sind nicht als Datenerhebung anzusehen.[263] Das „Speichern" ist nach § 3 Abs. 4 Satz 2 Nr. 1 BDSG nur das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger, das „zum Zwecke ihrer weiteren Verarbeitung oder Nutzung" erfolgt. Eine wichtige Form der Datenverarbeitung ohne gezielten Personenbezug wurde auch im bisherigen, jetzt aber entfallenen § 1 Abs. 3 BDSG geregelt, dort aber aus dem Anwendungsbereich des Gesetzes vollständig heraus genommen. Diese Rechtsfolge galt für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt werden und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden. Da die vorgeschlagene Regelung die erfassten Daten nicht aus dem Geltungsbereich des BDSG ausnimmt, sondern nur risikoadäquat regelt, verstößt sie auch nicht gegen den Regelungsvorbehalt des Art. 7 DSRL.[264]

Die Regelung zur sofortigen Löschung der verarbeiteten Daten unmittelbar nach Erfüllung dieser Zwecke ist erforderlich, um in einer Welt allgegenwärtiger Datenverarbeitung, in der tendenziell jede Handlung eine Datenspur hinterlassen kann, ein unbefangenes Handeln zu ermöglichen.[265] Sie ist zentrale Voraussetzung für die Rechtserleichterungen für diese Form der Datenverarbeitung. Diese Forderung entspricht § 4 Abs. 2 Nr. 2 TDDSG und § 13 Abs. 2 Nr. 2 MDStV sowie Art. 6 Abs. 1 des Entwurfs der Europäischen Kommission für eine neue Telekommunikationsdatenschutz-Richtlinie.[266]

3. Grundsätze der Datenverarbeitung

In die Informationsgesellschaft passt kein formelles Verbot der Informationsverarbeitung. Doch ist auch in der Informationsgesellschaft zu beachten, dass jede die Selbstbestimmung

---

259 Die Stellungnahme ist in Anhang 5, S. 278 ff. abgedruckt.

260 *BVerfGE* 100, 313 (366).

261 *OLG Bremen*, NJW 1993, 798.

262 *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7 Rn. 55.

263 So *Geiger*, in: *Simitis* u.a. BDSG, § 13 Rn. 10 für die zwangsläufige Kenntnisnahme von verschiedenen Aktivitäten der Bürger bei Außendienstterminen öffentlich Bediensteter; ebenso z.B. *Gola/Schomerus*, BDSG, § 13 Anm. 2; *Schaffland/Wiltfang*, BDSG, § 14 Rn. 3 m.w.N.

264 Sie kann europarechtlich mit dem berechtigten Interesse nach Art. 7 f) DSRL gerechtfertigt werden. Weitergehender dagegen *Petersen* 2000, 133f.

265 S. auch Teil 3 Kap. 3.5.2.

266 Vorschlag vom 12.7.2000, KOM(2000)385 – s. hierzu z.B. *Krader*, RDV 2000, 251.

der betroffenen Personen nicht berücksichtigende Verarbeitung personenbezogener Daten ein Eingriff in ihre Grundrechte ist. Eine Lösung des Problems könnte darin bestehen, dass statt der bisherigen Regelung des § 4 Abs. 1 BDSG eine gesetzliche Regelung den Eingriff erlaubt, wenn einfach gehaltene Erlaubnistatbestände und genau definierte Verarbeitungsgrundsätze erfüllt sind.

Die Grundsätze sollten grundsätzlich nicht zwischen öffentlichem und nicht öffentlichem Bereich unterscheiden.[267] Keine Unterscheidung zwischen öffentlichem und nicht öffentlichem Bereich treffen ebenfalls das österreichische Bundesgesetz über den Schutz personenbezogener Daten,[268] das Schweizerische Bundesgesetz über den Datenschutz,[269] das portugiesische Datenschutzgesetz,[270] das finnische Datenschutzgesetz[271] und das schwedische Datenschutzgesetz.[272]

Wird einer der Grundsätze verletzt, ist die Datenverarbeitung unzulässig und rechtswidrig, mit den Rechtsfolgen des Löschungsanspruchs, der Unzulässigkeit ihrer Verwertung und Schadensersatzansprüchen.

3.1 Zulässigkeit der Datenverarbeitung

Datenschutz sollte bisher dadurch gewährleistet werden, dass der Gesetzgeber durch präzise Erlaubnistatbestände den Zweck und Umfang der Datenverarbeitung festlegt und dadurch vorab und abstrakt-generell die Datenverarbeitung kontrolliert. Die Fülle der bereichsspezifischen Regelungen im öffentlichen Bereich und die privaten Verarbeitungsordnungen im nicht öffentlichen Bereich haben im Wesentlichen die Verarbeitung personenbezogener Daten nicht eingeschränkt, sondern in breitem Umfang ermöglicht. Zugleich haben sie zur Unübersichtlichkeit, Unverständlichkeit und Zersplitterung des Datenschutzrechts beigetragen. Dieser Weg kann angesichts der Zunahme und Komplexität der künftigen Datenverarbeitung nicht weiterverfolgt werden.[273]

Nach dem hier vorgeschlagenen Ansatz soll Datenschutz dagegen nicht mehr in erster Linie durch die gesetzgeberische Kontrolle von Erlaubnistatbeständen, sondern vor allem durch Grundsätze für die Verarbeitung personenbezogener Daten gewährleistet werden. Den Gefährdungen der informationellen Selbstbestimmung, die in den Verarbeitungskontexten entstehen, ist durch Anforderungen entgegenzuwirken, die sich auf die Strukturierung der Verwendungszusammenhänge beziehen.[274] Nicht die abstrakte gesetzgeberische Zulassung der Datenverarbeitung, sondern Anforderungen an die Gestaltung der Informationszusammenhänge sollen in erster Linie den notwendigen Schutz gewährleisten. Sie sollen der betroffenen Person durch Transparenz, Nachvollziehbarkeit, Zweckbindung, Beschränkung auf das Erforderliche und Einwirkungsmöglichkeiten die nötigen Selbstdarstellungsmöglichkeiten sichern.[275] Sie sind gefährdungsabhängig umzusetzen und daher auch nicht darin zu unterscheiden, ob die Gefährdung im öffentlichen oder nicht öffentlichen Bereich ihren Ursprung hat, wenn auch in diesem die Grundrechte der verantwortlichen Stellen zu berücksichtigen sind.

---

267 S. Teil 2 Kap. 3.2.

268 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999.

269 Gesetz vom 19.6.1992 (Stand. 7.7.1998).

270 Gesetz Nr. 67/98 zum Schutz personenbezogener Daten vom 26.10.1998.

271 Datenschutzgesetz (523/1999) vom 22.4.1999.

272 Datenschutzgesetz (1998:204) vom 29.4.1998.

273 S. zur Kritik Teil 1 Kap. 1 und 4, zu Lösungsansätzen Teil 2 Kap. 3.

274 S. *BVerfGE* 65, 1 (44 ff.); 100, 313 (359).

275 Zu dieser Perspektive auch *Podlech* 1982, 451 ff; *Simitis* 1987, 1492; *Roßnagel* 1994, 227 ff.; *Albers* 2001, 233 ff.; *Trute* , in: *Roßnagel*, HB-Datenschutzrecht, Kap. 2.5 Rn. 32.

Doch auch im Rahmen dieser neuen Schutzstrategie ist aus europa- und verfassungsrechtlichen Gründen eine spezifische Legitimation des Grundrechtseingriffs notwendig. Dieser kann entweder über den individuellen Willen der betroffenen Person oder über den allgemeinen Willen der Rechtsgemeinschaft gerechtfertigt werden.

3.1.1 Vorrang der Selbstbestimmung

In einem modernen, die informationelle Selbstbestimmung schützenden Datenschutzgesetz muss allerdings die Einwilligung als Legitimationsgrund der Datenverarbeitung aufgewertet werden. Zugleich aber müssen – im Rahmen des Möglichen – Freiwilligkeit der Zustimmung und die Entscheidungsprärogative der betroffenen Person sichergestellt werden.[276] Die Einwilligung, nach § 183 BGB eine vorherige Zustimmung, ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung der betroffenen Person.[277] Auch im einfachen Datenschutzrecht muss die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen,[278] zur Grundregel werden.

Auch ist eine deutliche Entlastung des Datenschutzrechts, eine Einschränkung seiner Normenflut und Überdifferenzierung nur dadurch zu erreichen, dass die Zulässigkeit der Datenverarbeitung grundsätzlich an die Zustimmung der betroffenen Person geknüpft wird. Nicht in allen Fällen muss der Gesetzgeber die Konfliktlösung selbst festlegen, sondern sollte in vielen Fallkonstellationen eine Konfliktlösung der Parteien anregen und absichern.[279] Nur indem der Gesetzgeber die Datenverarbeitung von der Vereinbarung der Beteiligten abhängig macht, kann er auf viele Erlaubnistatbestände verzichten.

In dem neuen Datenschutzgesetz sollten die gesetzlichen Erlaubnistatbestände und die individuelle Einwilligung nicht mehr auf eine Stufe gestellt, sondern sollten unter eindeutigem Vorrang der Einwilligung jeweils für sich geregelt werden.[280] Auch Art. 7 a) DSRL nennt die Einwilligung an erster Stelle für eine Legitimierung der Datenverarbeitung. Ebenso nennt die Europäische Grundrechtecharta in Art. 8 Abs. 2 die Einwilligung der betroffenen Person vor der Möglichkeit eines gesetzlichen Erlaubnistatbestands. Auch in den neuen LDSG[281] und den meisten europäischen neuen Datenschutzgesetzen ist dies der Fall.

Eine Aufwertung der Einwilligung soll auch zu einer Datenschutzkommunikation zwischen verantwortlichen Stellen und den betroffenen Personen beitragen.[282] Mit P3P, dem Standard des W3C zur Datenschutzkommunikation im Internet, steht zumindest für diesen Bereich der Datenverarbeitung auch eine technische Lösung zur Verfügung.[283]

---

276 S. Teil 3 Kap. 3.3.

277 S. z.B. *Bizer* 1992, 139f.; *ders*., in: *Roßnagel*, RMD, § 3 TDDSG, Rn. 84; *Simitis*, in: *ders*. u.a., BDSG, § 4 Rn. 27; *Weichert*, in: HbCompR, Rn. 150; *Vogelgesang* 1987, 150; *Geiger*, NVwZ 1989, 37; *Podlech/Pfeiffer*, RDV 1998, 144; *Schulz* 1998, 62; *Kothe*, AcP 85 (1985), 110, 132; a. A. *Robbers*, JuS 1985, 928, 930; *Stern* 1994, § 86 I 5, die in der Einwilligung einen Grundrechtsverzicht sehen.

278 *BVerfGE* 65,1; s. hierzu auch *Engel-Flechsig*, in: *Roßnagel*, RMD, Einleitung zum TDDSG, Rn 23; *Simitis*, in: *ders. u.a*., BDSG, § 4 Rn. 27.

279 S. zu den Anforderungen um das hierfür notwendige Mindestmaß an Gleichberechtigung sicher zu stellen, Teil 3 Kap. 3.3.

280 So auch *Simitis*, DuD 2000, 721.

281 Ebenso § 11 DSG SH.

282 Die Zustimmungspflicht der Eltern zur Verarbeitung von Daten ihrer Kinder durch Internetanbieter nach dem Children's Online Privacy Protection Act (COPPA) von 1998 in den USA – s. z.B. www.ftc.gov/ogc/stat3.htm; s. hierzu auch die Children's Online Privacy Protection Rule vom Oktober 1999, die am 21.4.2000 in Kraft trat – www.cdt.org/privacy/childrensprivacy.pdf; s. hierzu auch *U.S. Federal Trade Commission* 1999, 5 – hat zu zusätzlichen Anstrengungen der Anbieter geführt, mit den Eltern in einen Kommunikationskontakt zu gelangen, um über ihre Privacy Policy zu unterrichten und die Zustimmung der Eltern einzuholen.

283 S. hierzu näher Teil 3 Kap. 3.2.3.

Nach Art. 11 Abs. 1 des italienischen Datenschutzgesetzes[284] ist die Datenverarbeitung verantwortlicher Stellen des Privatrechts oder öffentlicher Wettbewerbsunternehmen nur zulässig, wenn die betroffene Person ihre ausdrückliche, freiwillige und formgerechte Zustimmung erklärt hat.

Die Datenverarbeitung kann aber nicht nur auf die explizite Einwilligung der betroffenen Person gestützt werden. Vielmehr sollten zwei anderen Ausdrucksformen der Einwilligung als Erlaubnistatbestände ebenfalls die Datenverarbeitung zu legitimieren vermögen:

Im nicht öffentlichen Bereich ist ein *Vertrag* mit der betroffenen Person oder aus ein auf deren Initiative hin zustande gekommenes[285] *vertragsähnliches Vertrauensverhältnis* der Einwilligung gleichgestellt werden. Der Vertrag oder das vertragsähnliche Vertrauensverhältnis bestimmen ebenso wie die Einwilligung die Zweckbindung der Daten[286] und beschränken die Datenverarbeitung auf das für die Zweckerreichung Erforderliche.[287] Dies entspricht der Regelung des Art. 7 b) DSRL.

Im öffentlichen Bereich ist als Einwilligungsersatz anzusehen, wenn der Bürger sich mit einem *Antrag* oder einem sonstigen Anliegen freiwillig an die öffentliche Verwaltung wendet.[288] Er bringt damit zum Ausdruck, dass er mit allen Datenverarbeitungen einverstanden ist, die für die (datensparsame) Bearbeitung seines Antrags oder Anliegens erforderlich sind. Dies erstreckt sich auch auf die Weitergabe von Daten an Dritte, wenn die betroffene Person ein bestimmtes Verwaltungshandeln will, das nur erfüllt werden kann, indem die Daten an Dritte übermittelt werden. Auch diese Legitimation der Datenverarbeitung ist als Erlaubnistatbestand auszuformulieren.

3.1.2 Anwendungsbereiche der Einwilligung

Die Grundlage für die Verarbeitung personenbezogener Daten kann im *nicht öffentlichen* Bereich grundsätzlich nur der freie Wille der betroffenen Person sein. Als Grundsatz sollte daher ebenso wie umgekehrt für Informationsansprüche Privater gegenüber nicht öffentlichen Stellen[289] auch für die Verarbeitung personenbezogener Daten eine „Opt-in-Lösung“ gewählt werden. Im nicht öffentlichen Bereich bildet die Einwilligung somit die Hauptlegitimationsgrundlage der Datenverarbeitung.

Dies kann im *öffentlichen* Bereich so nicht der Fall sein. Hier ist die Verarbeitung an den gesetzlichen Befugnissen der Verwaltung zu orientieren. Im Bereich gebundener Verwaltung kann sich die Verwaltung kein Mehr an Eingriffsbefugnissen durch Einwilligung verschaffen, als ihr durch Gesetz zugestanden wird. Hier hat das Gesetz die Funktion einer die Freiheit des Einzelnen schützenden Grenze, die der Verwaltung vom Gesetzgeber gezogen wurde und deren Überwindung der Einzelne der Verwaltung nicht erlauben kann.

Allerdings begründet der Grundsatz der „Erforderlichkeit“[290] enge Schranken.[291] Häufig ergibt sich jedoch die Situation, dass Zusatzdaten die Arbeit der Behörden erleichtern, ohne dass bei deren Fehlen die Arbeitserledigung vereitelt würde: Klassisches Beispiel hierfür sind

---

284 Gesetz Nr. 675 vom 31.12.1996.

285 Damit soll ein – aus Sicht der betroffenen Person – aufgedrängtes Vertrauensverhältnis ausgeschlossen werden. Dies fordert Art. 7 b) DSRL, wenn dort die Datenverarbeitung nur „für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffene Person erfolgen“, für zulässig erklärt wird.

286 S. Kap. 3.5.

287 S. Kap. 3.4.

288 S. *Lamberg*, DÖV 1979, 894f.

289 S. zum Informationszugang zum öffentlichen Bereich Teil 2 Kap. 2.5.

290 S. Teil 3 Kap. 3.4.

291 S. Teil 3 Kap. 3.4.1.

zusätzliche Erreichbarkeitsdaten eines betroffenen Bürgers. Die Vereinfachung und Beschleunigung von Arbeitsabläufen kann es in verschiedenen Zusammenhängen wünschenswert machen, Zusatzdaten zu erhalten, die nicht im strengen Sinn erforderlich sind. In diesen Fällen sollte es zulässig sein, auf der Basis der Freiwilligkeit die betroffenen Bürger um eine Einwilligung in die Datenverarbeitung zu bitten.[292] Um allerdings zu verhindern, dass öffentliche Stellen über die Einwilligung ihre Verarbeitungsbefugnisse nach eigenem Belieben ausdehnen, muss auch für die Datenverarbeitung auf der Grundlage einer Einwilligung eine Grenze gezogen werden. Diese ergibt sich aus dem Grundsatz der Gesetzmäßigkeit der Verwaltung. Danach dürfen auch auf der Grundlage einer Einwilligung nur solche Daten verarbeitet werden, die zur Aufgabenerfüllung der öffentlichen Stelle geeignet und bestimmt (also zumindest nützlich) sind. Daten, die in keinem Zusammenhang mit der gesetzlichen Aufgabenerfüllung stehen, dürfen auch auf der Grundlage einer Einwilligung nicht verarbeitet werden.[293]

Für Einwilligungen gegenüber der Verwaltung gelten die weiter unten dargestellten Wirksamkeitsvoraussetzungen.[294] Danach darf kein Zweifel an der Freiwilligkeit der Einwilligung bestehen. Dies dürfte im Bereich gebundener Verwaltung regelmäßig die Bitte um zusätzliche Angaben ausschließen, wenn diese etwa für die Prüfung des Bestehens oder Nichtbestehens eines geltend gemachten Anspruchs nicht erforderlich sind. Die erforderlichen Datenpreisgaben müssen sich aus einem Erlaubnistatbestand ergeben. Für gesetzlich geregelte Entscheidungen kommt daneben keine Datenverarbeitung auf der Grundlage einer Einwilligung in Betracht.[295]

Im nicht gebundenen Bereich – zum Beispiel im eigenen Wirkungskreis der Gemeinde[296] oder im Kontext einer transparenten und informierenden Verwaltung[297] – bestehen grundsätzlich keine Bedenken, wenn die Verwaltung die Möglichkeit nutzt, sich die Datenverarbeitung durch die Einwilligung der betroffenen Person legitimieren zu lassen.[298]

3.1.3 Verarbeitungserlaubnis im öffentlichen Bereich

In vielen Fällen muss aber auch eine unfreiwillige Datenverarbeitung möglich sein. Als Erlaubnistatbestand für die zwangsweise Datenverarbeitung sollte für den öffentlichen Bereich vorgesehen werden, dass die Datenverarbeitung „zur Erfüllung einer gesetzlich zugewiesenen und in der Zuständigkeit der öffentlichen Stelle liegenden bestimmten Aufgaben erforderlich“ ist.[299] Dieser Erlaubnistatbestand entspricht inhaltlich den Generalklauseln der §§ 13 Abs. 1 und 14 Abs. 1 BDSG und damit der derzeit geltenden allgemeinen Regelung. Im Gegensatz zum geltenden Recht soll diese Regelung aber nicht gegenüber ihren vielen bereichsspezifischen Wiederholungen subsidiär sein, sondern diese überflüssig machen. Dadurch erhält der Erlaubnistatbestand eine erheblich größere Reichweite und eine weitergehende Bedeutung. Dieser Erlaubnistatbestand ist zwar sehr allgemein, erscheint aber aus mehreren Gründen vertretbar.

---

[292] S. *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7, Rn. 34.

[293] S. *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7, Rn. 35.

[294] Teil 3 Kap. 3.3.1.

[295] S. *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7, Rn. 38.

[296] S. z.B. *Lamberg*, DÖV 1979, 894 ff.

[297] S. z.B. *Roßnagel* 2000a, 257 ff.

[298] In bestimmten Bereichen wird dies bereits nach geltendem Recht gefordert. Zum Beispiel dürfen sogenannte Wahlhelferdateien, die regelmäßig die Grundlage für die Bestellung von Wahlvorständen bilden, ohne Zustimmung der Betroffenen nicht mit Personaldaten von öffentlich Bediensteten gespeist werden.

[299] Dies entspricht Art. 7 e) DSRL: Wahrnehmung einer Aufgabe im öffentlichen Interesse und in Ausübung öffentlicher Gewalt. Neben der Aufgabenzuweisung verweisen auf die behördliche Zuständigkeit auch Art. 16 Abs. 1 BayDSG; § 11 Abs. 1 Satz 1 HDSG; § 8 Abs. 1 DSG MV.

Sein von der sprachlichen Fassung her weiter Geltungsbereich wird durch das Erforderlichkeitsprinzip deutlich eingeschränkt.[300] Vor allem aber ist er im Kontext eines anderen Regelungskonzepts zu sehen. Datenschutz soll nicht mehr vorrangig durch eine vom Gesetzgeber vorab festgelegte präzise Beschreibung erlaubter Datenverarbeitungen gewährleistet werden,[301] sondern vor allem durch Datenverarbeitungsregeln, die möglichst weitgehend eine Kontrolle und Beeinflussung der Datenverarbeitung durch die betroffene Person sicherstellen. Die Datenverarbeitung wird somit nicht nur von der Erfüllung eines allgemeinen Erlaubnistatbestands abhängig gemacht, sondern vorwiegend von der Einhaltung Selbstbestimmung unterstützender Verarbeitungsanforderungen.

Die automatisierte Verarbeitung personenbezogener Daten ist in der Verwaltung schon derzeit selbstverständlich und wird zur notwendigen Grundlage einer elektronischen Verwaltung. Es wäre widersprüchlich, der Verwaltung eine Aufgabe zuzuweisen, die nur mit Hilfe der Verarbeitung personenbezogener Daten erfüllt werden kann, ohne ihr die Möglichkeit zu geben, dieses zu tun. Dies ist der tiefere Grund dafür, warum der Gesetzgeber alle Verarbeitungserfordernisse und nahezu alle Verarbeitungswünsche der Verwaltung in bereichsspezifischen Erlaubnistatbeständen anerkannt hat. Hinsichtlich der Frage des „Ob" der Datenverarbeitung bringt die Forderung, die Datenverarbeitung müsse immer bereichsspezifisch zugelassen werden, keinen Gewinn für den Datenschutz, der nicht auch durch die Anwendung des Erforderlichkeitsprinzips erreicht werden könnte. Die informationelle Selbstbestimmung wird nicht dadurch besser geschützt, dass der Gesetzgeber in einem bereichsspezifischen Gesetz präzisiert, dass die Datenverarbeitung zur Erfüllung der Verwaltungsaufgabe „X" zulässig ist. Daher kann diese Frage der Zulässigkeit auch in einer Generalklausel allgemein an die Aufgabenerfüllung und die Erforderlichkeit hierfür gebunden werden. Die hier vorgeschlagene Fassung der Datenverarbeitungserlaubnis im öffentlichen Bereich ermöglicht, zusammen mit dem Verzicht auf die Subsidiarität des BDSG, auf viele bereichsspezifische Regelungen zu verzichten, die den erforderlichen Aufgabenbezug der Datenverarbeitung nur – auf den jeweiligen Verwaltungsbereich konkretisiert – wiederholen.

Allerdings ist auch das „Wie" der Datenverarbeitung zu regeln. Denn es darf von einer Aufgabe nicht unmittelbar auf eine Befugnis geschlossen werden, ein spezifisches Mittel, hier eine bestimmte Form oder Phase der Datenverarbeitung, einzusetzen. In vielen bereichsspezifischen Regelungen werden daher auch spezifische Befugnisse, Anforderungen, Verfahren und Pflichten der Datenverarbeitung geregelt. Diese werden in vielen bereichsspezifischen Regelungen jedoch ähnlich oder gleich geregelt. Aus diesem Grund wird die Art und Weise der Datenverarbeitung in dem hier vorgeschlagenen Konzept – im Grundsatz und in modernisierter Form – nicht mehr durch bereichsspezifische Regelungen bestimmt, sondern durch die hier näher beschriebenen Anforderungen an die Datenverarbeitung. Sie werden für die Mehrzahl der bereichsspezifischen Regeln allgemein geregelt und damit „vor die Klammer gezogen". Dies entlastet die bereichsspezifischen Regelungen und macht das Datenschutzrecht normenklarer, übersichtlicher und verständlicher.[302] Diese Entlastungschance würde vergeben, würde für jede Datenverarbeitung durch öffentliche Stellen eine spezifische Regelung zur Art und Weise der Datenverarbeitung gefordert.[303]

Die hier vorgeschlagene Regelung macht bereichsspezifische Regelungen jedoch keineswegs überflüssig. Diese bleiben erforderlich, wenn sie zusätzliche Anforderungen – etwa in besonders sensitiven Bereichen vorsehen oder Ausnahmen enthalten, die zur Erreichung eines ge-

---

300 S. Teil 3 Kap. 3.4.

301 S. zur Kritik an diesem Konzept eines Datenschutzes durch vorlaufende gesetzgeberische Kontrolle Teil 1 Kap. 2.4.

302 Zur verfassungsrechtlichen Zulässigkeit s. Teil 2 Kap. 4.3.

303 Für mehr Freiräume und die Verwendung von Generalklauseln auch *Bull* 1998, 30 ff.; *Bäumler* 1998, 3.

setzlichen Ziels als erforderlich angesehen werden. Spezifische Regelungsbedürfnisse, insbesondere zur Absicherung der informationellen Selbstbestimmung gegenüber spezifischen Gefährdungen müssen weiterhin der Gegenstand bereichsspezifischer Regelungen sein. Sie sind daher notwendig, wenn die Zwecke, Formen und Mittel der Datenverarbeitung eine besondere Eingriffstiefe erreichen (Beispiele: Strafverfolgung, Gefahrenabwehr, Beobachtung politischer Bestrebungen, verdeckte Erhebung, Datenabgleich, Datenmitteilungen, Datenpool, Rasterfahndung).[304] Allerdings ist die Grenze zwischen eher alltäglichen und besonders eingriffsintensiven Verarbeitungsvorgängen schwer zu bestimmen.[305] Ein wichtiger Anhaltspunkt dafür dürfte sein, in welchem Maß die Datenverarbeitung gegen den Willen der betroffenen Person durchgesetzt werden muss: Je stärker dies der Fall ist, desto umfassender und präziser muss der Gesetzgeber die Datenverarbeitung regeln. Es wird die Aufgabe der weiteren Gesetzgebung in den einzelnen Bereichen der Datenverarbeitung sein, diese besonders eingriffsintensiven Zwecke, Mittel und Formen der Datenverarbeitung zu erkennen und sich auf diese zu konzentrieren. Diese Aufgabe wird durch den hier vorgeschlagenen Erlaubnistatbestand nicht überflüssig.

Oder anders ausgedrückt, um auf eine erhobene Befürchtung noch deutlicher einzugehen: Die hier vorgeschlagene Generalklausel ist nicht dafür gedacht, die differenzierten Regelungen zu einzelnen Instrumenten und Verfahren der Datenerhebung, Datenspeicherung, Datenorganisation und Datenübermittlung in bereichsspezifischen Regelungen einzuebnen. Die vorgeschlagene Regelung ersetzt daher zum Beispiel nicht die spezifischen Anforderungen im Recht der Gefahrenabwehr, der Strafverfolgung und der Geheimdienste oder im Sozial- und Gesundheitsbereich. Hier soll es im Wesentlichen bei den bestehenden Befugnisregelungen zum Eingriff in das Recht auf informationelle Selbstbestimmung und den bestehenden Sicherungen dieses Grundrechts bleiben.[306]

Die Generalklausel wäre zu allgemein und – trotz der sie ergänzenden Anforderungen zur Datenverarbeitung – mit den Anforderungen des Volkszählungsurteils nicht vereinbar, wenn für die Verarbeitung allgemeine Aufgabenbeschreibungen wie die polizeiliche Generalklausel oder eine allgemeine Vorsorgeregelung ausreichen würden. In diesen Fällen würde die Verweisung auf die gesetzliche Aufgabenregelung keine klaren Konturen aufweisen, die es – trotz des Erforderlichkeitsprinzips – der betroffenen Person ermöglichen würden, die sie betreffende Datenverarbeitung abzusehen.[307] Diese sich bereits aus den verfassungsrechtlichen Grundlagen des Datenschutzes[308] ergebende Schlussfolgerung kann verdeutlicht werden, wenn in dem Erlaubnistatbestand durch den Bezug auf eine „bestimmte“ Verwaltungsaufgabe die Rechtfertigung der Datenverarbeitung durch eine ganz allgemeine Aufgabenzuschreibung ausgeschlossen wird. Der allgemeine Erlaubnistatbestand für öffentliche Stellen könnte etwa wie folgt lauten:

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist zulässig, soweit dies zur Erfüllung gesetzlich zugewiesener und in der Zuständigkeit der öffentlichen Stelle liegender bestimmter Aufgaben erforderlich ist.

Das italienische Datenschutzgesetz[309] erlaubt in Art. 27 die Datenverarbeitung öffentlicher Stellen ausschließlich, wenn dies erforderlich ist um die ihnen durch Gesetz übertragenen

---

304 S. hierzu näher *Simitis* 1990, 487 ff.; *Simitis*, in: *ders*., BDSG, § 1 Rn. 197; s. hierzu auch *Petersen* 2000, 144.

305 Ebenso *Simitis*, in: *ders*., BDSG, § 1 Rn. 197.

306 S. hierzu bereits Teil 2 Kap. 3.1.

307 S. hierzu auch Teil 2 Kap. 4.1.

308 *BVerfGE* 65, 1 (44 ff.).

309 Gesetz Nr. 675 vom 31.12.1996.

Aufgaben zu erfüllen – unter Berücksichtigung sonstiger gesetzlicher Beschränkungen.[310] Die anderen Erlaubnistatbestände des Art. 7 DSRL werden nicht auf öffentliche Stellen angewandt.[311]

3.1.4 Verarbeitungserlaubnis im nicht öffentlichen Bereich

Im Gegensatz zum öffentlichen Bereich kann die Grundlage für die Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich grundsätzlich nur die Willensfreiheit der betroffenen Person sein. Grundsätzlich sollte daher eine „Opt-in-Lösung" gewählt werden: Die Datenverarbeitung setzt die vorherige Einwilligung der betroffenen Person voraus.[312]

Damit kann auch ein Wertungswiderspruch des geltenden Datenschutzrechts beseitigt werden: Während das BDSG der betroffenen Person zur Unterbindung einer Nutzung oder Übermittlung ihrer Daten zu Zwecken der Werbung, der Markt- oder Meinungsforschung nur ein Widerspruchsrecht einräumt,[313] setzen die Regelungen des Telekommunikations- und Online-Datenschutzrechts für eine Verwendung zu Zwecken der „Werbung, Kundenberatung oder Marktforschung" die Einwilligung des betroffenen Kunden voraus.[314] Diese Anerkennung der Entscheidungsbefugnis des betroffenen Vertragspartners führt auf das Grundmodell des Vertragsrechts zurück: Die Rechte einer Partei gegenüber der anderen können nicht über das hinausgehen, was diese ihr konkret zugestanden hat.[315] Eine Vereinheitlichung des Datenschutzrechts auf hohem Niveau[316] sollte diesen Ansatz der beiden für die moderne Datenverarbeitung beispielgebenden Rechtsbereiche verallgemeinern. Er entspricht auch der Regelung des Art. 6 Abs. 3 des Entwurfs einer neuen Telekommunikationsdatenschutz-Richtlinie.

Aber auch im nicht öffentlichen Bereich muss eine Datenverarbeitung ohne Einwilligung der betroffenen Person möglich sein. Zur Umschreibung dieser Ausnahmefälle ist allerdings der bisher die Datenverarbeitung steuernde Begriff des „berechtigten Interesses" zu weit. An ihn werden keine hohen Anforderungen gestellt. Als „berechtigtes Interesse" gilt „jedes von der Rechtsordnung gebilligte Interesse",[317] jedes „nach vernünftigen Erwägungen durch die Sachlage gerechtfertigtes, also ein tatsächliches Interesse, das wirtschaftlicher oder ideeller Natur sein kann"[318] oder sogar „jedes Interesse, das nicht gegen rechtliche Grundsätze ... verstößt".[319]

Ähnlich erlaubt Art. 7 f) DSRL den Mitgliedstaaten, die Datenverarbeitung zuzulassen, wenn das berechtigte Interesse des Datenverarbeiters oder eines Dritten, dem die Daten übermittelt werden, die geschützten Interessen überwiegt. Hier gilt „jedes Interesse, das nicht gegen rechtliche Grundsätze ... verstößt" als berechtigt.[320] Art. 7 DSRL verlangt jedoch von den Mitgliedstaaten nicht, den vorgegebenen Rahmen für Erlaubnistatbestände auszunutzen. Vielmehr sind Einschränkungen gegenüber Art. 7 DSRL zulässig. Allerdings darf der Daten-

---

310 Auf diese könnten sich die bereichsspezifischen Regelungen des öffentlichen Rechts beschränken.

311 S. zur Übermittlung Kap. 3.5.4.

312 So auch Art. 11 des italienischen Datenschutzgesetzes, Gesetz Nr. 675 vom 31.12.1996.

313 Während in allen anderen Bereichen die Einwilligung – oft sogar zusätzlich – eingeholt wird, um das Risiko der unzulässigen Datenverarbeitung auszuschließen, wird eine Einwilligung soweit wie möglich vermieden, wenn es um die werbliche Ansprache des Kunden geht; s. zum Widerspruchsrecht *Gola*, DuD 2001, 278; *Gola/Wronka*, RdA 1996, 217.

314 § 89 Abs. 7 Satz 1 TKG; § 5 Abs. 2 TDDSG; § 14 Abs. 2 MDStV.

315 *Bizer*, DuD 2001, 276f.

316 S. Teil 2 Kap. 3.3.

317 *Schaffland/Wiltfang*, § 28 Rn. 85.

318 *Gola/Schomerus*, § 28 Rn. 7.1; *Auernhammer*, § 28 Rn. 18.

319 *Dammann/Simitis*, Art. 7 Rn. 12.

320 *Dammann/Simitis*, Art. 7 Rn. 12.

verkehr mit anderen Mitgliedstaaten nicht erschwerten Bedingungen unterworfen werden. Dies ist nicht der Fall, wenn für die Datenverarbeitung in Deutschland strengere Anforderungen gestellt werden, die Datenverarbeitung in anderen Mitgliedstaaten davon aber nicht betroffen ist. Für Übermittlungen ins Ausland oder aus dem Ausland bedarf es allerdings einer Sonderregelung, die Art. 1 Abs. 2 DSRL gerecht wird.[321]

Der Begriff der „berechtigten Interessen" ermöglicht nahezu jede von der verantwortlichen Stelle gewünschte Datenverarbeitung. Er widerspricht damit dem Konzept der Entscheidungsprärogative der betroffenen Person. Dieses wird auch nicht dadurch erfüllt, dass die verantwortliche Stelle ihre berechtigten Interessen in einer offenen Abwägung ohne jeden Abwägungsmaßstab gegen die schutzwürdigen Interessen der betroffenen Person abwägt. Die weitere Verwendung dieses Begriffs würde eine grundsätzliche Opt-in-Lösung ad absurdum führen.

Die ohne Einwilligung der betroffenen Person zulässige Datenverarbeitung muss also eingeschränkt werden. Vom Schutzzweck des Gesetzes her, der betroffenen Person die Wahrnehmung ihres Grundrechts auf informationelle Selbstbestimmung zu gewährleisten, muss die verantwortliche Stelle im Regelfall dessen Entscheidung abwarten und respektieren. Nur im Ausnahmefall, wenn ihr diese Rücksichtnahme ohne Verletzung eigener gewichtiger Interessen nicht zumutbar ist, soll sie auch gegen seinen Willen Daten verarbeiten dürfen. Dabei ist zu berücksichtigen, dass Datenverarbeitungen, die wegen der Offenkundigkeit oder der Art der Verarbeitung schutzwürdige Interessen der betroffenen Person offensichtlich nicht beeinträchtigen können und durch die personenbezogene Daten aus allgemein zugänglichen Quellen erhoben werden, ohnehin zulässig sein sollen.[322] Von dieser Grundkonstellation der Interessenabgrenzung her, bietet es sich an, die Bestimmung des Erlaubnistatbestands an dem Gedanken der privaten Rechtsverfolgung und Gefahrenabwehr zu orientieren.[323]

Statt diesen Erlaubnistatbestand in einem Begriff (wie etwa „rechtlich anerkannte Interessen") zusammenzufassen, sollte seine Steuerungskraft dadurch erhöht werden, dass er in Anlehnung an Art. 7 DSRL spezifiziert wird:[324]

Auch ohne Einwilligung der betroffenen Person ist die Verarbeitung personenbezogener Daten zulässig, wenn dies erforderlich ist, um

1. *eigene Rechte der verantwortlichen Stelle oder Rechte Dritter zu schützen oder zu verfolgen,*
2. *Verpflichtungen, die durch Rechtsvorschrift der verantwortlichen Stelle auferlegt wurden, zu erfüllen oder*
3. *eine Gefahr für Leben, Gesundheit oder sonstige bedeutende Rechtsgüter der betroffenen Person abzuwehren, für die diese ihre Einwilligung nicht erteilen kann, weil es ihr tatsächlich oder rechtlich nicht möglich ist oder sie geistesgestört ist.*

Für drei spezielle Bereiche der Datenverarbeitung sollten weitere ihren Arbeitsbedingungen angepasste Erlaubnistatbestände und Verarbeitungsregelungen ermöglicht werden, wenn diese Bereiche sich selbst Verhaltensregeln erarbeiten, die von den zuständigen Kontrollstellen an-

---

321 S. hierzu Teil 2 Kap. 5.

322 S. Teil 3 Kap. 2.2.

323 Diese Anregung stammt aus dem Gespräch mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

324 Nr. 1 entspricht in einer – dem neuen Konzept entsprechenden – einengenden Weise Art. 7 f) DSRL, Nr. 2 Art. 7 c) DSRL und Nr. 3 Art. 7 d) DSRL.

erkannt werden können.[325] Das BDSG sollte nur allgemeine Vorgaben für diese selbstgesetzten – und konstitutiv wirkenden – Verhaltensregeln treffen. Diese sollten für

- Warndienste, Detekteien und Auskunfteien, die Daten zum Schutz oder zur Durchsetzung von Rechten Dritter durch Weitergabe an diese verarbeiten, regeln dürfen, dass die Datenverarbeitung auch ohne Einwilligung im erforderlichen Umfang, im Rahmen der Verhältnismäßigkeit, auf der Basis belastbarer und für den Schutz oder Aufklärungszweck relevanter Daten, unter technisch-organisatorischer Sicherung der Zweckbindung[326] und zur erforderlichen Weitergabe an berechtigte Empfänger erfolgen darf. In den Verhaltensregeln sind angemessene Prüf- und Löschpflichten vorzusehen.[327]
- Unternehmen und Hilfsunternehmen der Medien, die Daten ausschließlich für eigene journalistisch-redaktionelle, künstlerische oder literarische Zwecke verarbeiten, regeln dürfen, dass die Datenverarbeitung auch ohne Einwilligung nach Kriterien hoher journalistischer Sorgfalt unter technisch-organisatorischer Sicherung der Zweckbindung[328] erfolgen darf. Die Verhaltensregeln können vorsehen, dass die Unterrichtung und die Rechte der betroffenen Personen so weit eingeschränkt werden, wie dies zum Erreichen der Verarbeitungszwecke unerlässlich ist. Sie können die Aufsicht über die Datenverarbeitung statt einer staatlichen Kontrollstelle einer ebenso wirksamen Selbstverwaltungseinrichtung übertragen.[329]
- Forscher, die für die wissenschaftliche Forschung erforderliche Datenverarbeitungen durchführen, regeln dürfen, dass die Verarbeitung personenbezogener Daten auch ohne Einwilligung erfolgen darf, wenn das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens erheblich ist, der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und schutzwürdige Interessen der betroffenen Person nicht verletzt werden.[330] Die Datenverarbeitung muss so durchgeführt werden, dass die Zweckbindung[331] technisch-organisatorisch gesichert ist und die Daten zum frühest möglichen Zeitpunkt anonymisiert oder, wenn dies nicht möglich ist, pseudonymisiert werden und die hierfür erforderlichen Vorsorgemaßnahmen[332] eingehalten werden.[333]

---

325 S. Teil 3 Kap. 6.5.

326 S. hierzu Teil 3 Kap. 3.5.3 a.E.

327 S. hierzu z.B. *Weichert*, DuD 2001, 264 ff.; *Duhr*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.5.

328 S. Teil 3 Kap. 3.5.3 a.E.

329 S. zum Datenschutz für die Presse *Schulz/Korte* AfP 2000, 530; *dies*., KritV 2001, 113; *Kloepfer*, AfP 2000, 511.

330 Für die Durchführung des Forschungsvorhabens muss kein „erhebliches" Überwiegen des Forschungsinteresses über die Interessen der betroffenen Person mehr nachgewiesen werden. Vielmehr genügt es, dass deren gegenüber dem Forschungsvorhaben und den mit ihm verbundenen Risiken schutzwürdiges Interesse nicht verletzt wird. Hierfür kann berücksichtigt werden, dass die Forschung in der Regel kein Interesse an einer Intervention in die Sphäre der betroffenen Person hat Andererseits ist das Interesse der betroffenen Person ausreichend geschützt, da es ein tatsächlich schutzwürdiges Interesse nicht durch überwiegende Interessen überwunden werden kann. Ohne die konturenlose Abwägung eines „Überwiegens" völlig unterschiedlicher Interessen wird es für beiden Seiten einfacher vorhersagbar, ob eine Zweckänderung ohne Einwilligung der betroffenen Person zulässig ist – in ähnlicher Zielrichtung hat die bisherige Kommentarliteratur die Anforderung des „Überwiegens" streng ausgelegt – s. z.B. *Dammann*, in: *Simitis u.a*., BDSG, § 14 Rn. 54; *Gola/Schomerus*, BDSG, § 5 Anm. 3.1; *Wedde*, in: *Däubler/Klebe/Wedde*, BDSG, § 14 Rn. 6.

331 S. Teil 3 Kap. 3.5.3 a.E.

332 S. Teil 3 Kap. 3.4.3.

333 S. hierzu z.B. *Bizer* 1992, 190 ff.; *ders*., DuD 1999, 392; *Simitis* 1987, 1475; *Gerling*, DuD 1999, 384; *ders*., in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.11; *Mayen*, NVwZ 1997, 446; *Tinnefeld*, DuD 1999, 35.

Für alle anderen Verarbeitungszwecke gilt das Opt-in-Prinzip,[334] das entweder eine vorherige Einwilligung, einen Vertrag oder ein vertragsähnliches Vertrauensverhältnis voraussetzt. Dies betrifft vor allem die nicht vereinbarte oder gebilligte Änderung des Verarbeitungszwecks oder die Übermittlung von Daten und damit insbesondere zum Beispiel die Zwecke der Markt- und Meinungsforschung, der Werbung und des Marketing,[335] den Handel mit Adressen oder das Veröffentlichen von Verzeichnissen. Diese Zwecke liegen zwar im berechtigten unternehmerischen Interesse der verantwortlichen Stelle, doch vermag dieses nicht zu rechtfertigen, in seiner Verfolgung die Entscheidungsprärogative der betroffenen Person zu übergehen oder gar zu missachten. Es bleibt den verantwortlichen Stellen – ganz im Sinn der Marktwirtschaft – überlassen, für ihr Anliegen – unter Darlegung ihrer Datenschutzmaßnahmen – zu werben und die betroffene Person zu gewinnen, ihnen die Verarbeitung ihrer Daten zu erlauben oder gar mit ihnen vertraglich zu vereinbaren. In der Wirtschaft gelten in vielen Bereichen Opt-in-Lösungen bereits als „professionell". So heißt es zum Beispiel für die Gewinnung von Daten jenseits von vertraglich erforderlichen Daten etwa für Werbung und Marketing: „Kunden- und wettbewerbsorientiert handelnde Datenschutzverantwortliche werden generell auf die Anwendung transparenter Opt-in-Prozeduren hinwirken".[336]

Ein Anspruch auf Datenverarbeitung oder Zweckänderung ergibt sich auch nicht aus Art. 5 Abs.1 GG für veröffentlichte Daten, für die bisher die Privilegierung des § 28 Abs. 1 Nr. 3 und Abs. 2 BDSG gilt, da die Informationsfreiheit nur den Informationszugang und die Informationsaufnahme schützt,[337] nicht aber eine sich anschließende Verarbeitung und kommerzielle Nutzung der Daten. Die Verarbeitung veröffentlichter Daten ist auch nicht im Katalog der Erlaubnistatbestände des Art. 7 DSRL enthalten. Für besonders schützenswerte Daten wird die Datenverarbeitung von Art. 8 Abs. 2 e) DSRL nur erlaubt, wenn die betroffene Person die Daten offenkundig selbst öffentlich gemacht hat.

Für die Daten, die vor Inkrafttreten der neuen Regelungen rechtmäßig verarbeitet worden sind, müssen geeignete Übergangsregelungen vorgesehen werden.[338]

Das italienische Recht[339] vermeidet ebenfalls eine Generalklausel und sonstige Abwägungserfordernisse. In enger Anlehnung an Art. 7 DSRL[340] beschränkt es die Ausnahmen von der Einwilligungspflicht auf einzeln aufgeführte Tatbestände. Für die Verarbeitung von Daten über Wirtschaftsaktivitäten, die unter anderem zum Zweck der kommerziellen Kommunikation, der Werbung, des Marketing oder Marktuntersuchungen oder interaktiver Untersuchungen über kommerzielle Kommunikation erhoben worden sind, läßt es Art. 12 des Datenschutzgesetzes jedoch genügen, wenn die betroffene Person hierüber und über ihr Widerspruchsrecht informiert worden ist.[341] Auch das portugiesische Datenschutzgesetz[342] orientiert sich in Art. 6 eng an den Erlaubnistatbeständen des Art. 7 DSRL. Vergleichbares gilt für Schedule 2 des

---

334 Eine Ausnahme besteht für die Datenverarbeitung, durch die wegen der Offenkundigkeit oder der Art der Verarbeitung schutzwürdige Interessen der betroffenen Person offensichtlich nicht beeinträchtigt werden – s. Teil 3 Kap. 2.2.

335 S. zur Begründung oben im Text.

336 *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4 Rn. 10.

337 S. Teil 3 Kap. 2.2.

338 S. Teil 3 Kap. 10.

339 S. Art. 12 des italienischen Datenschutzgesetzes, Gesetz Nr. 675 vom 31.12.1996.

340 Abweichungen enthält das italienische Datenschutzgesetz vor allem in Form einer Privilegierung der Daten aus öffentlich zugänglichen Quelle und der Daten über wirtschaftliche Aktivitäten. Diese sind in Art. 7 DSRL nicht vorgesehen. Insofern ergeben sich Bedenken gegen die italienische Regelung.

341 S. hierzu auch die Widerspruchsregelung in Art. 13 Abs. 1 e) – s. hierzu Teil 3 Kap. 6.4.

342 Gesetz Nr. 67/98 zum Schutz personenbezogener Daten vom 26.10.1998.

britischen Data Protection Acts 1998[343] und für Section 10 des schwedischen Datenschutzgesetzes.[344] Das finnische Datenschutzgesetz[345] nimmt in Section 8 auch die Erlaubnistatbestände des Art. 7 DSRL zur Grundlage, konkretisiert diese aber zum Beispiel für die Datenverarbeitung in Arbeitsverhältnissen, im Zahlungsverkehr und in der Kundendatenverarbeitung.

3.1.5 Verarbeitung besonders schützenswerter Daten

Die besondere Schutzwürdigkeit personenbezogener Daten kann in der Regel nicht abstrakt, sondern nur aus dem jeweiligen Verarbeitungskontext heraus bestimmt werden. Abstrakte Listen besonders schützenswerter Daten,[346] wie sie Art. 8 DSRL enthält, sind für den Datenschutz eher kontraproduktiv. Dennoch muss die Vorgabe des Art. 8 DSRL umgesetzt werden. Sie lässt sich damit rechtfertigen, dass die Wahrscheinlichkeit bei diesen Daten größer als bei anderen Daten ist, dass ihre Verarbeitung Interessen der betroffenen Person beeinträchtigt.[347]

Für die Verarbeitung besonders schützenswerter Daten im Sinn des Art. 8 DSRL genügen weder eine allgemeine Einwilligung noch die allgemeinen Erlaubnistatbestände. Vielmehr sollte die Datenverarbeitung nur zulässig sein, wenn die betroffene Person ausdrücklich in die Verarbeitung dieser Daten eingewilligt hat[348] oder wenn die Verarbeitung ausdrücklich in einem Gesetz zugelassen ist, das die Daten, die Verarbeitungsschritte, besondere Schutzgarantien und einen spezifischen Tatbestand eines besonderen öffentlichen Interesses an dieser Datenverarbeitung nennt.[349]

Das Niederländische Datenschutzgesetz[350] sieht in Art. 16 ein grundsätzliches Verbot der Verarbeitung besonders schützenswerter Daten vor, für das in den Art. 17 bis 22 nach Arten der Daten geordnet ausführliche spezifische Verarbeitungsermächtigung an einzelne Adressaten wie Religionsgemeinschaften, Gewerkschaften, politische Parteien oder im Gesundheitsbereich Tätige geregelt werden. Art. 23 enthält abschließend eine Wiederholung der Erlaubnistatbestände des Art. 8 DSRL. Ebenso regelt Section 13 des schwedischen Datenschutzgesetzes[351] ein Verbot der Datenverarbeitung und erteilt in den Sections 14 bis 19 Erlaubnisse für bestimmte Verwendungszusammenhänge wie den Gesundheitsbereich, die Forschung oder Arbeitsverhältnisse. In vergleichbarer Weise werden die besonders schützenswerten Daten durch Schedule 2 des britischen Data Protection Acts 1998[352] und durch Section 11 und 12 des finnischen Datenschutzgesetzes[353] geschützt. Nach Section 12 (2) des finnischen Gesetzes muss die Notwendigkeit einer Speicherung der Daten spätestens alle fünf Jahre überprüft werden. In vielen europäischen Gesetzen sind außerdem Regelungen enthalten, die der Regierung oder Kontrollstellen die Befugnis übertragen, weitere Fälle öffentlichen Interesses zu benennen, die eine Verarbeitung besonders schützenswerter Daten rechtfertigen.

---

343 Data Protection Act vom 18.7.1998.

344 Datenschutzgesetz (1998:204) vom 29.4.1998.

345 Datenschutzgesetz (523/1999) vom 22.4.1999.

346 S. zu diesen kritisch *Simitis* 1994, 484 ff.

347 S. Teil 3 Kap. 2.2.

348 Zu den weiteren Voraussetzungen der Einwilligung s. Teil 3 Kap. 3.3.

349 S. näher Teil 3 Kap. 3.1.5.

350 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

351 Datenschutzgesetz (1998:204) vom 29.4.1998.

352 Data Protection Act vom 18.7.1998.

353 Datenschutzgesetz (523/1999) vom 22.4.1999.

Das schweizerische Bundesgesetz über den Datenschutz[354] fordert in Art. 18 Abs. 2, dass die Erhebung besonders schützenswerter Daten der betroffenen Person erkennbar sein muss. Verarbeitet werden dürfen diese Daten nach Art. 17 Abs. 2 nur, wenn ein Gesetz dies ausdrücklich vorsieht oder dies für eine gesetzlich „klar umschriebene Aufgabe" unentbehrlich ist, der Bundesrat es bewilligt hat oder die betroffene Person eingewilligt hat. Eine Übermittlung ist nach Art. 12 nicht ohne besondere Rechtfertigung zulässig, als die Art. 13 eine Einwilligung, ein Gesetz oder ein überwiegendes privates oder öffentliches Interesse nennt. Durch ein Abrufverfahren dürfen besonders schützenswerte Daten nach Art. 19 Abs. 3 nur zugänglich gemacht werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht.

Strenger regelt das italienische Datenschutzgesetz[355] den Umgang mit besonders schützenswerten Daten. Nach Art. 22 erfordert deren Verarbeitung eine schriftliche Einwilligung der betroffenen Person, die durch die Kontrollstelle bestätigt werden muss. Durch die Bestätigung soll verhindert werden, dass die Zustimmung aufgrund von Abhängigkeiten oder Machtungleichgewichten faktisch erzwungen wird. Die Kontrollstelle soll die Bestätigung innerhalb von 30 Tagen erteilen. Geschieht dies nicht innerhalb dieser Frist, gilt der Antrag als abgelehnt. Mit der Bestätigung oder danach kann die Kontrollstelle angemessene Maßnahmen oder Vorkehrungen zum Schutz der Daten fordern. Im öffentlichen Bereich ist die Datenverarbeitung nur zulässig, wenn sie ausdrücklich in einem Gesetz zugelassen ist, das die Daten, die Verarbeitungsschritte und einen spezifischen Tatbestand eines besonderen öffentlichen Interesses an dieser Datenverarbeitung nennt. Fehlt eine solche gesetzliche Erlaubnis, kann die öffentliche Stelle bei der Kontrollstelle beantragen, unter den Aktivitäten zur Erfüllung gesetzlicher Aufgaben diejenigen zu bestimmen, die spezifische Tatbestände eines besonderen öffentlichen Interesses an dieser Datenverarbeitung begründen. Ausnahmen können außerdem für die Strafverfolgung und den Gesundheitsbereich vorgesehen werden.

3.2 Transparenz der Datenverarbeitung

Informationelle Selbstbestimmung setzt voraus, dass die Datenverarbeitung gegenüber der betroffenen Person transparent ist. Sie muss in der Lage sein, sich zu informieren, „wer was wann und bei welcher Gelegenheit über sie weiß".[356] Nur wenn ihr die Datenverarbeitung bekannt ist, kann sie ihre Rechtmäßigkeit überprüfen und ihre Rechte in Bezug auf die Datenverarbeitung geltend machen. Dies gilt für alle Phasen der Datenverarbeitung. Ohne Transparenz wird die betroffene Person faktisch rechtlos gestellt. Daher nennt das Bundesverfassungsgericht als verfahrensrechtliche Schutzvorkehrung des Grundrechts auf informationelle Selbstbestimmung Aufklärungs- und Auskunftspflichten.[357]

3.2.1 Erhebung der Daten bei der betroffenen Person und Unterrichtung

An dem Grundsatz, dass die personenbezogenen Daten bei der betroffenen Person zu erheben sind, sollte festgehalten werden. Dadurch wird die Verarbeitung dieser Daten und deren Intention der Person bekannt. Sofern ihr die Informationen nicht durch die Erhebung oder aus anderen Gründen bereits vorliegen, ist die betroffene Person über

- die verantwortliche Stelle sowie den für die Datenverarbeitung Verantwortlichen oder den Datenschutzbeauftragten,
- Art, Umfang und Zwecke der Verarbeitung,
- die Rechtsgrundlage der Verarbeitung oder die Freiwilligkeit der Angaben,

---

354 Gesetz vom 19.6.1992 (Stand. 7.7.1998).

355 Gesetz Nr. 675 vom 31.12.1996.

356 *BVerfGE* 65, 1 (43).

357 *BVerfGE* 65, 1 (46).

- die möglichen Folgen einer Verweigerung der Angaben,
- den Empfängerkreis bei beabsichtigten Übermittlungen,
- ihre Rechte nach diesem Gesetz sowie
- ihre Wahl- und Gestaltungsmöglichkeiten

zu unterrichten, soweit dies nicht aufgrund der Umstände unangemessen ist.[358] Der Inhalt der Unterrichtung sollte von der betroffenen Person jederzeit abgerufen oder angefordert werden können.

Durch die Unterrichtung wird eine aktive Mitwirkung der betroffenen Person ermöglicht, die entweder die Daten selbst liefert, die Erhebung ausdrücklich duldet oder sich ihr entzieht.[359] Die Verletzung der Unterrichtungspflicht macht die Erhebung der Daten rechtswidrig und verhindert rechtlich eine weitere Verarbeitung. Diese ist nur auf der Basis einer hierauf bezogenen Einwilligung möglich.[360]

Die Unterrichtung der betroffenen Person ist eine fortwährende Pflicht, die immer dann aktuell wird, wenn eine Datenverarbeitung stattfinden soll, über die noch keine Unterrichtung stattgefunden hat.[361] Die betroffene Person sollte immer über den aktuellen Stand der sie betreffenden Datenverarbeitung informiert sein.

Langfristig sollte diese Anforderung an die steigende Verbreitung der Internetnutzung bei verantwortlichen Stellen und betroffenen Personen angepasst werden. Die zunehmende Verfügbarkeit nahezu kostenloser komfortabler Übertragungsmöglichkeiten und sehr sicherer Kryptographie ermöglicht es, betroffene Personen detaillierter und häufiger über sie betreffende Datenverarbeitungen zu unterrichten und sie damit stärker zu Teilnehmern der Datenverarbeitung zu machen. Dabei geht es nicht darum, sie über jeden „Verarbeitungsschritt" zu unterrichten, sondern ihnen die sie interessierenden Veränderungen in der Datenverarbeitung mitzuteilen. Dabei könnte Frequenz und Detaillierungsgrad auch nach Interesse der betroffenen Person variieren, soweit sich der Aufwand in vertretbaren Grenzen hält. Zwar erfordert dies insbesondere bei verantwortlichen Stellen ein Umdenken und auch eine teilweise Umstellung ihrer Verarbeitungsprozesse und lädt ihnen damit zumindest für eine Übergangsfrist auch zusätzliche Kosten auf. Mittel- und langfristig entsteht aber ein großer Gewinn: Durch die damit einher gehende größere Transparenz der Datenverarbeitungsprozesse für die betroffenen Personen wird einerseits die Akzeptanz wachsen und es werden dadurch erweiterte Geschäftsmodelle in der „Informationswirtschaft" möglich. Andererseits dient die regelmäßige Unterrichtung der Aktualität und Korrektheit der Daten für die verantwortliche Stelle. Wird eine erweiterte Unterrichtungspflicht gegenüber allen am Internet angeschlossenen betroffenen Personen an den Zeitpunkt gekoppelt, zu welchem das entsprechende Datenverarbeitungsverfahren sowieso geändert werden muss – etwa wenn neue Anforderungen aus dem Anwendungskontext heraus entstehen oder Daten auf neue technisch-organisatorische Strukturen transferiert werden sollen –, dann geschieht sie ohne große zusätzliche Belastung der verantwortlichen Stellen und ist damit auch verhältnismäßig.

Nach dem Grundsatz der Informationpflicht der Safe Harbor Principles muss eine Organisation Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an

---

358 Die meisten dieser Angaben werden durch Art. 10 DSRL gefordert.

359 *Geiger*, in: *Simitis u.a.*, BDSG, § 13 Rn. 33.

360 Ähnlich bezüglich der Verletzung der Belehrungspflicht nach § 101 Abs. 1 Satz 2 AO 1977, *BFH*, RDV 1991, 143; s. hierzu auch *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 46.

361 S. auch Art. 6 Abs. 4 sowie Erwägungsgrund 15 des Entwurfs der Europäischen Kommission für eine neue Telekommunikationsdatenschutz-Richtlinie, KOM(2000)385 – s. hierzu z.B. *Krader*, RDV 2000, 251.

welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Die Daten sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern.[362]

Das italienische Datenschutzgesetz[363] fordert in Art. 10 Abs. 1 eine mündliche oder schriftliche Unterrichtung über Zweck sowie Art und Weise der Datenverarbeitung, über die freiwillige oder unfreiwillige Natur der Datenanforderung, die Konsequenzen einer Weigerung, die Empfänger oder Kategorien der Empfänger einer Übermittlung oder Verbreitung der Daten, die Rechte der betroffenen Person sowie die Identität der verantwortlichen Stelle.

3.2.2 Unterrichtung bei sonstiger Erhebung

Ohne Mitwirkung der betroffenen Person sollten personenbezogene Daten nur erhoben werden dürfen, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder der zulässige Verarbeitungszweck[364] eine solche Erhebung erforderlich macht. Zur Sicherung der Verhältnismäßigkeit dieser Verpflichtung sollte sie unter den Vorbehalt eines unverhältnismäßigen Aufwands gestellt werden. Diese Verhältnismäßigkeitsklausel sollte ihrerseits nicht unter einen konturenlosen Abwägungsvorbehalt gestellt werden. Zum Einen ist eine Berücksichtigung der Interessen der betroffenen Person bereits im Verhältnismäßigkeitsprinzip angelegt. Zum Anderen sollte statt einer offenen Abwägung durch die verantwortliche Stelle gefordert werden, dass die betroffene Person baldmöglichst unterrichtet wird. Aufgrund dieser Information kann sie sich dann gezielt gegen eine ihr rechtswidrig erscheinende Verarbeitung wehren.

Werden Daten nicht bei der betroffenen Person erhoben, ist diese – soweit noch sinnvoll – über die gleichen Umstände zu unterrichten, wie bei einer Datenerhebung bei ihr selbst.[365] Auch diese Unterrichtung ist eine fortdauernde Pflicht. Ohne sie ist die Datenverarbeitung rechtswidrig. Eine entsprechende Regelung könnte sich an § 3 Abs. 5 TDDSG und § 12 Abs. 6 MDStV orientieren. Eine Unterrichtung der betroffenen Person hat vor der Speicherung oder der ersten Übermittlung zu erfolgen.

Angesichts der gesellschaftlichen Bedeutung elektronischer Kommunikation ist eine Harmonisierung der datenschutzrechtlichen Pflicht zur Unterrichtung mit den nach dem TDG 1997, nach dem Entwurf eines TDG 2001,[366] dem MDStV und dem Fernabsatzgesetz bestehenden Pflichten zur Anbieterkennzeichnung und zur Information des Verbrauchers[367] nach Inhalt und Begrifflichkeit anzustreben. Unter den Bedingungen elektronischer Kommunikationsmöglichkeiten ist nicht nachvollziehbar, warum die nach dem Verbraucherrecht für Anbieter geltenden Informationspflichten ohne nennenswerte Ausnahmen gelten, aber die datenschutzrechtliche Benachrichtigung durch viele Ausnahmetatbestände zum seltenen Regelfall wird.[368] Daher muss es genügen, die verantwortlichen Stellen generell von der Unterrichtungspflicht zu befreien, wenn die Unterrichtung unmöglich ist oder einen unverhältnismäßi-

---

362 S. Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 11.

363 Gesetz Nr. 675 vom 31.12.1996.

364 S. Teil 3 Kap. 3.3.1.

365 S. hierzu Art. 11 DSRL.

366 S. Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EEG), BT-Drs. 14/6098.

367 Anbieterkennzeichnung nach § 6 TDG und § 6 MDStV, Unterrichtung des Verbrauchers nach § 2 FernAG und die Informationspflichten nach Art. 5 und 6 EG-E-Commerce-Richtlinie.

368 S. *Bizer*, DuD 2001, 275.

gen Aufwand erfordert.[369] Auf die beiden generellen Ausnahmen kann sich nur berufen, wer diese der Kontrollstelle vorab gemeldet hat.

Ausnahmen von der Unterrichtungspflicht sollten zurückhaltend vorgesehen werden, da sie zum Einen für die betroffene Person ausschließen, ihre Rechte wahrzunehmen. Zum Anderen verkomplizieren sie das Datenschutzrecht unnötig. Sie sollten in bereichsspezifischen Gesetzen nur für bestimmte Behörden des Sicherheitsbereichs, der Nachrichtendienste, der Strafverfolgung und der Finanzverwaltung vorgesehen werden. Allgemein sollten Ausnahmen von der nachträglichen Unterrichtung vorgesehen werden, sofern sie unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde, den zulässigen Verarbeitungszweck der verantwortlichen Stelle erheblich gefährden würde oder die Datenverarbeitung ausschließlich der Datensicherung oder Datenschutzkontrolle dient.

Keine individuelle Unterrichtungspflicht sollte für die Datenverarbeitung ohne gezielten Personenbezug[370] gelten. Sie allein führt nur zu geringen Risiken für die betroffene Person. Für die verantwortliche Stelle, die in der Regel nicht einmal genau weiß, welche Daten sie ungezielt verarbeitet, wäre die vorherige Unterrichtung eine unangemessene bürokratische Belastung, ohne dass sie den Datenschutz substanziell fördert. An die Stelle der individuellen Unterrichtung, sollte eine allgemeine Datenschutzerklärung treten.[371] Diese Ausnahme dürfte mit Art. 10, 11 Abs. 1 und 13 DSRL vereinbar sein, zumindest wenn die Argumentation zum Ausschluss der Auskunft nach § 19 Abs. 2 BDSG auch auf diese Ausnahme von der Unterrichtungspflicht übertragen wird. In diesem Fall ist die Ausnahme durch die ansonsten unverhältnismäßige Belastung der verantwortlichen Stelle nach Art. 13 Abs. 1 g) DSRL gerechtfertigt worden.[372] Wichtiger erscheint jedoch die Argumentation, dass die vorgesehene Unterrichtung durch eine Datenschutzerklärung die einzig praktikable Unterrichtung in einer Welt allgegenwärtiger Datenverarbeitung sein wird.

Nach den Safe Harbor Principles muss eine Organisation, die die betroffene Person nicht bereits bei der Erhebung der Daten informiert hat, dies so bald wie möglich nachholen, auf jeden Fall aber bevor sie die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben und verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.[373]

Das italienische Datenschutzgesetz[374] fordert in Art. 10 Abs. 3 eine Unterrichtung der betroffenen Person vor der Speicherung oder der ersten Übermittlung. Ausnahmen sollen nach Abs. 4 nur gelten, wenn die Kontrollstelle festgestellt hat, dass die Erfüllung der Informationspflicht unmöglich oder im Vergleich zum geschützten Recht der betroffenen Person offensichtlich unverhältnismäßig ist. Nach Abs. 4 werden nur zwei Ausnahmen zugelassen, nämlich die Unmöglichkeit der Informationspflicht oder ihre offensichtliche Unverhältnismäßigkeit im Vergleich zum geschützten Recht der betroffenen Person. Auf die Ausnahme kann sich nur derjenige berufen, für den die Kontrollstelle das Vorliegen der Ausnahmegründe im konkreten Fall anerkannt hat.

---

369 S. auch § 26 LDSG Schleswig-Holstein und Art. 10 Abs. 4 des italienischen Datenschutzgesetzes, Gesetz Nr. 675 vom 31.12.1996.

370 S. Teil 3 Kap. 2.6.

371 S. hierzu den folgenden Abschnitt.

372 S. hierzu BT-Drs. 14/4329, 40.

373 S. den Grundsatz der Informationspflicht, Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 11; Entscheidung der Kommission vom 26.7.2000, Erwägungsgrund 5, EG-ABl. L 215 vom 25.8.2000, 7.

374 Gesetz Nr. 675 vom 31.12.1996.

3.2.3 Datenschutzerklärung und Datenschutzkommunikation

Alle verantwortlichen Stellen sollten – als Teil ihres Datenschutzmanagementsystems[375] – verpflichtet werden, eine allgemein zugängliche Datenschutzerklärung zu veröffentlichen.[376] In dieser sollten sie ihre Datenverarbeitungs- und Datenschutzpraxis darstellen und auch über die „Logik ihrer Datenverarbeitung" unterrichten. Die Datenschutzerklärung ist den Änderungen der Datenverarbeitungs- und Datenschutzpraxis ständig anzupassen, um diese korrekt wiederzugeben. Die Datenschutzerklärung ist in der „Offline-Welt" an gut zugänglichen Plätzen zu veröffentlichen. Für alle verantwortlichen Stellen, die im WWW vertreten sind, ist die Datenschutzerklärung auf der Website an leicht erreichbarer Stelle zu publizieren.[377] Für die verantwortlichen Stellen, die im elektronischen Geschäftsverkehr tätig sind, muss eine vergleichbare Regelung ohnehin entsprechend Art. 10 Abs. 2 der Electronic-Commerce-Richtline geschaffen werden. Nach dieser Vorschrift muss der Diensteanbieter alle einschlägigen Verhaltenskodizes, denen er sich unterwirft, sowie Links auf diese im Internet angeben. Wenn beim „Besuch" der Website auf die Datenschutzerklärung ausdrücklich hingewiesen wird und sie jederzeit aufrufbar ist, könnte sie für die über das WWW initiierte Datenverarbeitung die individuelle Unterrichtung ersetzen.

Aufgeschlossene Unternehmen benutzen bereits heute Privacy Statements als Grundlage für eine transparente Darstellung ihrer Datenschutzpolitik zur Vertrauenswerbung in der Öffentlichkeit. Datenschutzerklärungen entsprechen dem internationalen Stand der Transparenz im Datenschutz.[378] Sie werden von den Safe Harbor Principles,[379] von den selbstregulierten Datenschutzprogrammen in den USA,[380] den privaten Siegel-Programmen zum Datenschutz[381] und auch vom künftigen allgemeinen Datenschutzgesetz Japans gefordert.[382]

Die Regelung zur Datenschutzerklärung könnte etwa den folgenden Inhalt haben:

Eine verantwortliche Stelle, die geschäftsmäßig personenbezogene Daten automatisiert verarbeitet, erstellt eine Erklärung über

1. *die Verarbeitung personenbezogener Daten,*
2. *die Struktur und Funktionsweise ihrer Verfahren,*
3. *eine Übersicht über ihre Datenschutz- und Datensicherungsmaßnahmen,*
4. *die Rechtsordnung, die für eine Datenverarbeitung im Ausland Anwendung findet,*
5. *die Verhaltensregeln, denen sie sich unterworfen hat, samt deren Inhalt sowie*

---

375 S. Teil 3 Kap. 4.1.

376 Zu einer ähnlichen Idee der zu veröffentlichenden „Informations- und Kommunikationspläne" s. z.B. *Albers* 1996, 136; s. zur Datenschutzerklärung auch *Vogt/Tauss* 1998, Nr. 8.

377 Als ein international genutztes Hilfsmittel zu ihrer Erstellung, das allerdings mit den hier genannten Datenschutzanforderung nicht völlig übereinstimmt, kann der OECD Privacy Statement Generator angesehen werden – s. zu diesem http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

378 S. z.B. *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4 Rn. 52; *Grimm/Roßnagel*, DuD 2000, 448f.

379 S. den Grundsatz der Informationspflicht, Grundsätze des „sicheren Hafens" zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 11.

380 S. z.B. Online Privacy Alliance – www.privacyalliance.org/resources/ppguidelines.shtml; Prinzipien für die amerikanische Internet-Werbewirtschaft der Network Advertising Initiative (NAI) vom Juli 2000, www.ftc.gov/opa2000/07/onlineprofiling.

381 S. z.B. TRUSTe, www.truste.org; „BBBonline" von der Verbraucherschutzvereinigung Council of Better Business Bureaus (BBB), www.bbbonline.org; „WebTrust" von den Organisationen der Wirtschaftsprüfer in USA und Kanada American Institute of Certified Public Accountants und Canadian Institute of Chartered Accountants (CPA), www.cpawebtrust.org; „ESRB Privacy Online" von dem Entertainment Software Rating Board (ESRB), www.esrb.org.

382 Japanische Expertenkommission 2000, 6f., 9.

6. *ihr Beschwerdeverfahren und eine jederzeit erreichbare Telekommunikationsverbindung für Beschwerden*

und macht die Erklärung öffentlich zugänglich, soweit dies ohne Offenlegung eines geschützten Geheimnisses möglich ist. Statt des geschützten Geheimnisses ist sein Inhalt so ausführlich darzustellen, wie dies ohne Preisgabe des Geheimnisses möglich ist. Soweit möglich sollte die Erklärung in einer nach dem Stand der Technik maschinenlesbaren Form veröffentlicht werden.

Das Publizieren einer Datenschutzerklärung im WWW eröffnet die Möglichkeit, den weltweiten Datenschutzstandard des W3C „Platform for Privacy Preferences (P3P)" für eine Datenschutzkommunikation zwischen datenverarbeitender Stelle und betroffener Person zu nutzen.[383] Der ursprüngliche Entwurf von P3P sah vor, dass Nutzer und Anbieter ihre Vorstellungen von Verhaltensregeln frei aushandeln und anschließend die Daten nach den vereinbarten Regeln austauschen. Das wurde für einen ersten Implementierungsschritt als zu schwierig angesehen und zunächst auf ein reines Verfahren für „Notice and Choice" abgespeckt.[384] In dieser Form kann P3P zwar einen Abgleich der Datenschutzvorstellungen zwischen verantwortlicher Stelle und betroffener Person durchführen und die betroffene Person vor unzumutbaren Bedingungen warnen. Diese kann aber nur entscheiden, ob sie die Bedingungen akzeptiert oder die Kommunikation abbricht. Eine Kommunikation über Datenschutzbedingungen ermöglicht dieser Standard derzeit noch nicht. Daher muss P3P zu einem echten Kommunikationsstandard fortentwickelt werden. Im Idealfall sollte er Verhandlungen darüber ermöglichen, wie die personenbezogenen Daten verwendet werden, ob und in welchem Umfang überhaupt personenbezogene Daten nötig sind und welche Pseudonyme verwendet werden. Diese Aushandlung sollte ebenso anonym möglich sein wie die späteren Transaktionen.

3.2.4 Transparenz der Struktur der Datenverarbeitung

Ebenso wichtig wie die Transparenz über die gespeicherten Daten dürfte die Transparenz über die Struktur der Datenverarbeitung und ihre Zwecksetzung sein. Dies ist zum Beispiel bei der Erstellung von Profilen wichtiger als die Transparenz über die einzelnen Daten, die in dem Profil zusammengeführt werden.[385] Wer geschäftsmäßig[386] personenbezogene Daten automatisiert verarbeitet, sollte daher verpflichtet sein, die Struktur der Datenverarbeitung in verständlicher Form zu veröffentlichen.

Diese Forderung ist für das deutsche Datenschutzrecht nicht völlig neu. So sind zum Beispiel bei automatisierter Personaldatenverarbeitung nach § 90g Abs. 5 BBG, § 56f Abs. 5 BRRG die Verarbeitungs- und Nutzungsformen automatisierter Personalverwaltungssysteme allgemein bekannt zu geben.

Art. 12 a) DSRL und ihm folgend § 6a Abs. 3 BDSG sehen eine Auskunft an die betroffene Person über „den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten" vor. Diese Auskunftspflicht könnte entfallen, wenn eine allgemeine Veröffentlichung in einer Datenschutzerklärung verpflichtend ist.

Die zu veröffentlichenden Daten sollten mit den Daten korreliert werden, die der betriebliche Datenschutzbeauftragte ohnehin aufnehmen muss oder die an die Kontrollstelle zu melden

---

383 S. z.B. *Cranor*, DuD 2000, 479; *Cavoukian/Gurski/Mulligan/Schwartz*, DuD 2000, 475; *Grimm/Roßnagel* 2000a, 293 ff.; *dies*. 2000b, 157; *Wenning/Köhntopp*, DuD 2001, 139 ff.; *Gress*, DuD 2001, 144 ff.

384 S. zur Entwicklung von P3P *Grimm/Roßnagel* 2000, 293 ff.

385 S. Teil 3 Kap. 3.5.4.

386 Dies bedeutet: regelmäßig, in gewissem Umfang, nicht notwendig mit der Absicht, Gewinn zu erzielen. Erfasst sind damit z.B. auch alle öffentlichen Stellen und alle gemeinnützigen Organisationen, auf die dieser Begriff zutrifft.

sind (Art. 18 DSRL), so dass sie in jeder verantwortlichen Stelle ohnehin vorliegen und nicht gesondert erhoben und erstellt werden müssen.

Für diese Erklärungspflicht ist der Schutz von Geschäfts- und Betriebsgeheimnissen zu berücksichtigen, da dieser von der Freiheit der Berufsausübung des Art. 12 Abs. 1 GG gefordert wird.[387] Außerdem enthält der Erwägungsgrund 41 der DSRL eine Präzisierung des Auskunftsrechts über den logischen Aufbau der automatisierten Verarbeitung: Danach darf das Auskunftsrecht weder das Geschäftsgeheimnis noch das Recht am geistigen Eigentum berühren. Dies darf allerdings nicht dazu führen, dass der betroffenen Person jegliche Information verweigert wird.

Vorbild für den Umgang mit Geschäfts- und Betriebsgeheimnissen könnten umweltrechtliche Genehmigungsverfahren sein.[388] Nach § 10 Abs. 2 BImSchG[389] muss der Antragsteller beispielsweise Geschäfts- und Betriebsgeheimnisse als solche deklarieren und in einem gesonderten Umschlag der Genehmigungsbehörde übergeben. In den auslegungsfähigen Unterlagen werden statt der Geschäfts- und Betriebsgeheimnisse Umschreibungen des Sachverhalts verwendet, die die Geschäfts- und Betriebsgeheimnisse nicht offenbaren. In diesem Zusammenhang wird darauf hingewiesen, dass es sich um Geschäfts- und Betriebsgeheimnisse handelt, die sich auf bestimmte Sachverhalte beziehen. Diese können dann nicht von der Öffentlichkeit, aber von der Genehmigungsbehörde überprüft werden. In der Datenschutzerklärung könnte in gleicher Weise der Sachverhalt umschrieben werden, ohne die Geschäfts- und Betriebsgeheimnisse zu offenbaren. Allerdings sollte darauf verwiesen werden, dass eine nähere Erläuterung nicht möglich ist, ohne Geschäfts- und Betriebsgeheimnisse zu offenbaren. Die Kontrollstelle kann dann im Rahmen ihrer Aufsichtstätigkeit überprüfen, ob diese Aussage zutrifft. Ist dies nicht der Fall, könnte sie eine Ergänzung der Datenschutzerklärung fordern. Keine Geschäfts- und Betriebsgeheimnisse können jedoch die Datenverarbeitung personenbezogener Daten als solche sowie die erhobenen Daten, die Zwecke der Datenverarbeitung und die vorgesehenen Empfänger von Datenübermittlungen sein. Die Frage des Geschäfts- und Betriebsgeheimnisses kann sich allenfalls auf bestimmte Aspekte der Struktur der Datenverarbeitung beziehen.

3.2.5 Individuelles Auskunftsrecht

Die betroffene Person hat nach Art. 12 DSRL außerdem ein umfassendes und effektives Auskunftsrecht. Dessen gesetzliche Umsetzung wird im Zusammenhang mit den Rechten der betroffenen Person beschrieben.[390]

3.2.6 Transparenz der Technik

Die allgemeine Forderung nach größerer Transparenz der Systeme der Informationstechnik wird auch durch den Aspekt des Datenschutzes unterstützt. Transparenz in diesem Sinn bedeutet, dass mit angemessenem Aufwand durchschaubar ist, was das System einschließlich aller Betriebs- und Anwendungssoftware genau tut. Wünschenswert ist, dass soweit wie irgend möglich die betroffenen Personen selbst oder zumindest von ihnen ausgewählte sachkundige Vertrauenspersonen hierzu in die Lage versetzt werden. Transparent müsste sein, was das System tun soll und was es wirklich tut, was es – auch über seine Schnittstellen mit anderen Systemen oder Menschen kommunizierend – tun kann und wie sich das System in der Zeit verändern kann. Systeme der Informationstechnik sind heutzutage außerordentlich kom-

---

387 S. hierzu z.B. *Koch*, MMR 1998, 461; *Eul*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.2.

388 S. hierzu z.B. auch § 225 des Entwurfs eines UGB, s. UGB-KOM-E 1998, 842 ff.

389 S. hierzu näher *Roßnagel*, in: *Koch/Scheuing*, GK-BImschG, § 10 Rn. 246 ff.

390 S. Teil 3 Kap. 7.1

plex und zumindest potenziell multi- wenn nicht nahezu allfunktional, so dass keine der Fragen hinlänglich als beantwortbar gelten kann.

Das wesentliche Hilfsmittel zur Herstellung der beschriebenen technischen Transparenz ist eine umfassende detaillierte Offenlegung aller „Innereien“: detaillierte Schaltpläne aller Hardware (natürlich in maschinenhantierbarer Form) und die kommentierten Quellcodes aller Programme, vom Betriebssystem bis zur Anwendungssoftware. Zusätzlich ist erforderlich, die Details aller Werkzeuge (z.B. Compiler) offenzulegen, die verwendet wurden, um Hard- und Software zu entwerfen und zu produzieren, sowie rekursiv dann wiederum alle Werkzeuge, die verwendet wurden, um die gerade genannten Werkzeuge zu entwickeln.[391] Wenn nicht gegenüber den betroffenen Personen selbst, so muss diese Offenlegung zumindest gegenüber den Prüfenden erfolgen, seien es Sicherheitszertifizierungsstellen, Datenschutzgutachter oder Kontrollstellen. Vorzugsweise sollte die Offenlegung in einer allgemein zugänglichen Veröffentlichung bestehen, da dies einerseits die Zahl der Prüfer und damit die Qualität des Prüfergebnisses (mehr Augen sehen mehr) und andererseits die Vertrauenswürdigkeit der Produkte selbst erhöht.[392] Diese vor mehr als einem Jahrzehnt erhobene Forderung mutete zunächst utopisch an, ihr wird aber in den letzten Jahren zumindest in Teilbereichen Rechnung getragen: Unter dem Schlagwort „Open Source“ hat ein Software-Entwicklungsmodell zunehmend auch wirtschaftliche Bedeutung erlangt, das auf der Offenlegung der Quellen[393] und einer Zerlegung in verständliche, wartbare Module sowie deren Auswahl durch die Gemeinschaft der Entwickler aufbaut.

Um eine ausreichende Transparenz der Datenverarbeitung sicher zu stellen, könnte für bestimmte Verarbeitungsformen oder -zwecke (wie der Verarbeitung von Gesundheits- oder Personaldaten) gesetzlich gefordert werden, dass ab einem bestimmten Zeitpunkt, die Verarbeitung personenbezogener Daten nur zulässig ist, wenn alle Quelltexte und Werkzeuge der Programme offen gelegt sind.[394]

Eine solche Forderung ließe sich jedoch allenfalls mit einer langen Übergangsfrist verfassungsrechtlich rechtfertigen, die mindestens die vollständige Abschreibung der zuletzt gekauften Systeme ermöglicht. Nur so könnte die Verhältnismäßigkeit der neuen Eigentumsinhaltsbestimmung gewährleistet werden. Außerdem ist diese Forderung mit Rechten am geistigen Eigentum abzugleichen. Für diese Forderung ist der Datenschutz allein ein unzureichender Hebel. Ob sie vertreten werden soll, ist eher eine Frage der Sicherheit der Informationstechnik und der Innovationssicherung in der IT-Industrie. Sollten diese Diskussionen zu einer gesetzlichen Regelung zur Offenlegung von Quelltexten führen, würde auch der Datenschutz davon profitieren.

---

391 Für die Etablierung von Offenlegungspflichten kann es sinnvoll sein, von hinten, also bei der Entwicklung von Soft- und Hardware zu beginnen: Zunächst wird gefordert, dass (zumindest) die Werkzeuge (z.B. Compiler, Entwicklungsumgebung etc.) dokumentiert und möglichst sogar allgemein offengelegt werden. Dies erlaubt eine klarere Dokumentation der Schnittstellen und berührt Geschäftsgeheimnisse weniger, als die Forderung nach Offenlegung der Quellcodes selbst. Bezüglich der Sicherheit brächte bereits die Dokumentation der Werkzeuge einen Fortschritt mit sich: Falls entdeckt wird, dass z.B. ein bestimmter Compiler „Trojanische Pferde“ in mit ihm übersetzte Programme einbaut, wäre feststellbar, welche Anwender hiervon betroffen sind. Die Dokumentation der verwendeten Werkzeuge verbunden mit ihrer weitest möglichen Offenlegung sollte als Minimalanforderung angesehen werden. Es wäre der erste Schritt auf einem langen Weg.

392 Beginnend im Bereich der Kryptographie, wo inzwischen allgemein akzeptiert ist, dass die Sicherheit nicht auf der Geheimhaltung des Algorithmus oder seiner Implementierung beruhen darf, ist unter Experten zunehmend unstrittig, dass dieses Prinzip auch für IT-Sicherheit allgemein gelten sollte und – aus Gründen der Vertrauenswürdigkeit der Sicherheit – auch zunehmend gelten muss.

393 Kombiniert mit unentgeltlicher Nutzbarkeit, welche nicht Gegenstand dieses Gutachtens ist.

394 S. zur Forderung nach transparenter Software auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.3.1999; *AK Technik* 2000.

Bis dahin sollte das moderne Datenschutzrecht allenfalls als Ziel formulieren, dass die verantwortlichen Stellen Systeme mit Open Source einsetzen sollen, soweit ihnen dies möglich und zumutbar ist. Darüber hinaus könnte der Einsatz von Systemen mit Open Source ein geeigneter Gegenstand für eine Zielfestlegung der Bundesregierung sein.[395]

Um eine ausreichende Kontrolle der Datenverarbeitung zu ermöglichen, sollte außerdem vorgesehen werden, dass die Kontrollstelle die für die verantwortliche Stelle verfügbaren Quelltexte prüfen darf. Soweit dies möglich ist, muss die verantwortliche Stelle für eine Kontrolle die Informationen beschaffen.

3.2.7 Besondere Transparenzanforderungen

Für bestimmte im BDSG zu regelnde Verarbeitungsformen sollten besondere Transparenzanforderungen formuliert werden wie zum Beispiel für

- mobile Datenverarbeitungsgeräte,[396]
- audiovisuelle Systeme,[397]
- biometrische Verfahren,[398]
- Verarbeitung von Personenprofilen.[399]

3.2.8 Transparenz und Kontrolle

Insgesamt sind die Transparenzanforderungen nicht in der Weise zu verstehen, dass der betroffenen Person künftig viele Prüfpflichten auferlegt werden, um ihre Rechte geltend zu machen. Auch für eine nachlässige und uninteressierte betroffene Person muss ein Mindestmaß an Datenschutz – vor allem durch Systemdatenschutz – gewährleistet sein. Auch muss sie sich auf eine gewisse Kontrolle durch Aufsichtsbehörden[400] oder Verbände[401] verlassen können. Allerdings setzt Mitwirkung und Selbstdatenschutz ein gewisses Mindestmaß an Kenntnis und Interesse hinsichtlich der Datenverarbeitung voraus. Die Transparenzanforderungen sollen diese ermöglichen. Dabei ist zu beachten, dass die Transparenzmaßnahmen zum Einen Anknüpfungspunkte für technische Kontrollverfahren wie P3P sein können und zum Anderen die Grundlage für die Tätigkeit vertrauenswürdiger Dritter, die für die betroffene Person prüfen.[402]

Transparenz lässt sich nämlich auch durch die Kontrolle Dritter herstellen. Dies widerspricht zwar der Forderung der jungen Internet-Generation, die sich selbst direkt informieren und dies nicht Dritten überlassen will. Wenn aber ansonsten die Information gar nicht bekannt gegeben werden könnte, weil eine allgemeine Transparenz auch immer Transparenz für Böswillige oder Konkurrenten bedeutet, liegt es im Interesse der betroffenen Person, wenn an ihrer Stelle ein vertrauenswürdiger Dritte die Struktur der Datenverarbeitung überprüfen kann.

3.3 Einwilligung in die Datenverarbeitung

Zur Gewährleistung der informationellen Selbstbestimmung soll die Zulässigkeit der Datenverarbeitung grundsätzlich an die Einwilligung der betroffenen Person geknüpft werden.[403]

---

395 S. Teil 3 Kap. 6.2.
396 S. Teil 3 Kap. 8.2.2
397 S. Teil 3 Kap. 8.2.1
398 S. Teil 3 Kap. 8.2.3.
399 S. Teil 3 Kap. 3.5.5.
400 S. Teil 3 Kap. 9.1.
401 S. Teil 3 Kap. 9.3.
402 Hier dürfte mit einer gewissen Professionalisierung wie in den USA zu rechnen sein.
403 s. Teil 3 Kap. 3.1.

Bisher garantiert die Möglichkeit der Einwilligung in vielen Fällen jedoch nicht die Entscheidungsprärogative der betroffenen Person, sondern erlaubt der verantwortlichen Stelle auf Grund ihrer Machtposition ihre Verarbeitungswünsche ohne Rücksicht auf die individuelle Situation der betroffenen Person durchzusetzen, indem sie ihre Einwilligung „erzwingt".[404] Die Einwilligung ist vielfach „der Schlüssel zu einem nahezu unbegrenzten, von allen ansonsten zu beachtenden gesetzlichen Schranken befreiten Zugang zu den ... jeweils gewünschten Angaben"[405] und Verarbeitungsformen. Die Einwilligung ratifiziert Verarbeitungserwartungen des Datenverarbeiters, auf die die betroffene Person weder Einfluss hat noch haben kann. Die freie Selbstbestimmung durch Einwilligung kann so leicht zur Fiktion werden.[406]

Die individuelle Einwilligung ist zwar unverzichtbar, aber teilweise nicht ausreichend. Wenn die Situation für den Einzelnen nicht hinreichend durchschaubar ist, er durch wirtschaftliche oder persönliche Unterlegenheit nicht frei entscheiden kann oder der Eingriff besonders gewichtig oder riskant ist, dann muss sein Selbstbestimmungsrecht durch zusätzliche Verfahren und Sachkriterien gesichert werden.[407]

3.3.1 Voraussetzungen der Einwilligung

Einerseits sind gesetzliche Vorgaben notwendig, um die Verwirklichungsbedingungen der Selbstbestimmung zu ermöglichen. Wie im Verbraucherschutzrecht ist dem sozial Schwächeren ein gewisser Grundschutz zu bieten. Statt einer formalen Autonomie muss das Datenschutzrecht die Selbstverwirklichungschance des Einzelnen schützen. Andererseits dürfen solche Regelungen nicht zur Bevormundung der betroffenen Person führen. Die gesetzliche Umhegung der Selbstbestimmung muss sich auf deren Schutz und Förderung beschränken. Ist sichergestellt, dass die betroffene Person umfassend über die beabsichtigte Datenverarbeitung informiert ist und völlig freiwillig in sie einwilligt, muss die Einwilligung grundsätzlich die Datenverarbeitung rechtfertigen können.

Um dies sicherzustellen, sollte die Wirksamkeit der Einwilligung von der Erfüllung der folgenden vier Voraussetzungen abhängig sein, die im Streitfall von der verantwortlichen Stelle nachzuweisen sind.[408]

1) Unterrichtung

Die Einwilligung kann nur dann auf der „freien Entscheidung" der betroffenen Person „beruhen", wenn diese weiß, worin sie einwilligt.[409] Die Einwilligung kann die beabsichtigte Verarbeitung der personenbezogenen Daten nur dann legitimieren, wenn die betroffene Person rechtzeitig und umfassend über sie informiert worden ist.[410] Die Unterrichtung der betroffenen Person muss genau so weit reichen wie der Anwendungsbereich der Einwilligung.[411] Die Einwilligung sollte in dem Umfang wirksam sein, in dem die betroffene Person zuvor über die für sie bedeutsamen Umstände der Datenverarbeitung unterrichtet worden ist. Sie muss sich beispielsweise je nach Bedeutung für die betroffene Person erstrecken auf

---

404 S. *Simitis*, JZ 1986, 188.

405 *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 20.

406 S. hierzu näher *Bergmann/Möhrle/Herb*, § 4 Rn. 34; *Schapper/Dauer*, RDV 1987, 170 m.w.N.; *Schapper/Dauer*, CR 1987, 497.

407 *Kothe*, AcP 85 (1985), 155 unter Hinweis auf BVerfGE 65, 1 (46), das mit gleichen Argumenten die Erforderlichkeit der Datenschutzbeauftragten zur effektiven Sicherung des Selbstbestimmungsrechts rechtfertigt.

408 S. z.B. *Däubler/Klebe/Wedde*, BDSG, § 4 Rn. 14.

409 *Gola/Schomerus*, BDSG, § 4 Rn. 5.5; *Fischer/Uthoff*, MedR 1996, 116; *Wohlgemuth*, BB 1996, 693.

410 S. ausführlich *Bizer*, in *Roßnagel*, RMD, § 3 TDDSG, Rn. 85.

411 Legislativer Ausdruck der informierten Einwilligung ist im geltenden Recht die Hinweispflicht in § 4 Abs. 2 Satz 1 BDSG, § 4a Abs. 1 Satz 2 BDSG-E sowie § 3 Abs. 6 TDDSG, § 12 Abs. 7 MDStV und § 47 Abs. 7 RStV.

- Umfang, Form und Zweck der Datenverarbeitung,
- mögliche Verknüpfungen mit anderen Datenbeständen und potenzielle Empfänger der Daten, insbesondere wenn diese in einem Staat außerhalb der Europäischen Union sitzen,
- die Freiwilligkeit der Einwilligung, die Möglichkeit einer Verweigerung und deren Folgen,
- die Entkopplung von Einwilligung und beantragter Vertrags- oder Verwaltungsleistungen[412] und
- die Widerruflichkeit der Einwilligung.

Die Unterrichtung muss nicht schriftlich erfolgen,[413] ihre Erfüllung kann aber in der Regel nur nachgewiesen werden, wenn sie schriftlich erfolgt ist. Erfolgt die Einwilligung auf einem Formular, sind die Anforderungen an die Bestimmtheit des Hinweises und der Einwilligungserklärung identisch.

2) Freiwilligkeit

Nach Art. 2 h) DSRL und § 4a Abs. 1 BDSG muss die Einwilligung der betroffenen Person auf ihrer freien Entscheidung beruhen.[414] Diese muss nach Art. 7 a) DSRL ohne jeden Zweifel vorliegen. Die Freiwilligkeit ist nicht nur zu verneinen, wenn staatlicher Zwang ausgeübt wird,[415] sondern immer dann, wenn aufgrund rechtlicher oder faktischer Abhängigkeiten die Entscheidungsmöglichkeiten wesentlich eingeschränkt sind[416] oder wenn ein – mehr oder weniger unwiderstehlicher – Anreiz zur Einwilligung gesetzt wird.[417] Dies ist jedenfalls dann zu vermuten, wenn die Einwilligung die Datenverarbeitung in dauerhaften Abhängigkeitsverhältnissen (z.B. Arbeits- oder Anstaltsverhältnis) legitimieren soll. Die Freiwilligkeit der Einwilligung ist umgekehrt immer dann zu vermuten, wenn die vertragliche Leistung oder die beantragte Entscheidung nicht von ihr abhängig gemacht wird.

Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Dies ist nur dann ausgeschlossen, wenn (weiter-)bestehende Vertragspflichten dem entgegenstehen.

3) Kopplungsverbot

Wenn die Einwilligung freiwillig sein soll, muss zwischen ihr und der erstrebten Verwaltungs- oder Vertragsleistung ein Kopplungsverbot bestehen.[418] Die für die Verwaltungs- und Vertragsleistung erforderliche Datenverarbeitung wird bereits auf gesetzlicher Grundlage ermöglicht. Die darüber hinausgehende Datenverarbeitung muss freiwillig sein. Die Einwilligung zur gesetzlich nicht legitimierten darüber hinausgehenden Datenverarbeitung darf nicht mit der Drohung der Leistungsverweigerung erzwungen werden. Auch in dieser Frage sollte sich das Datenschutzgesetz am Vorbild des Telekommunikations- und Multimediadaten-

---

412 S. *Schrader* 1999, 3.

413 S. *Dörr*, RDV 1992, 167.

414 Dies gilt auch für die bisherige Fassung des § 4 Abs. 1 BDSG – s. z.B. LG *Stuttgart*, DuD 1999, 295

415 So *Geiger*, NVwZ 1989, 37.

416 S. z.B. *Schmidt*, JZ 1974, 246; *Rothe*, DuD 1996, 594; *Schulz* 1998, 63; *Wohlgemuth*, BB 1996, 693, der dies bei einem Bewerbungsgespräch ausschließt.

417 Z.B. verneint das *LG Stuttgart*, DuD 1999, 295, die Freiwilligkeit einer Einwilligung bei Auslobung von Preisen von insgesamt 22.500 DM und eines Höchstpreises von 10.000 DM für das Ausfüllen eines Fragebogens.

418 Für die Telekommunikation bestimmen dies § 89 Abs. 10 TKG und § 3 Abs. 2 Satz 2 TDSV – s. hierzu bereits für § 3 Abs. 2 TDSV 1996 *Königshofen*, RDV 1997, 102. Für Teledienste, Mediendienste und Rundfunkveranstaltungen legt dies § 3 Abs. 3 TDDSG, § 12 Abs. 4 MDStV und § 47 Abs. 4 RStV ausdrücklich fest – s. hierzu näher z.B. *Bizer*, in: *Roßnagel*, RMD, § 3 TDDSG, Rn. 112 ff. - s. zur Forderung eines Kopplungsverbots auch *Simitis*, DuD 2000, 722.

schutzrechts orientieren und durch die Verallgemeinerung der Regelungen in § 89 Abs. 10 Satz 1 TKG, § 4 Abs. 3 TDDSG und § 12 Abs. 4 MDStV eine Vereinheitlichung des Datenschutzrechts auf hohem Niveau erreichen.

Zumindest für (Infrastruktur-)Leistungen der zivilisatorischen Grundversorgung (z.B. Telekommunikation, Internetzugang, Kranken- und Rentenversicherung, Girokonto, Kreditkarte, medizinische Behandlung) darf die Einwilligung in eine Datenverarbeitung zu anderen als die für die Vertragserfüllung erforderlichen Zwecke zur Voraussetzung gemacht werden.[419] Für diese ist daher zu fordern, dass jeweils immer auch eine nicht diskriminierende Alternative angeboten wird, die ohne zusätzliche (zu der für die Vertragsabwicklung notwendige) Verarbeitung personenbezogener Daten auskommt (Beispiel: SCHUFA-freies Girokonto auf Guthabenbasis). Durch selbstgesetzte Verhaltensregeln[420] sollte festgelegt werden, welcher Datensatz für einen bestimmten Vertragstyp zur vertraglichen Datenverarbeitung erforderlich ist. Dabei muss es ein Ziel des Systemdatenschutzes sein, für die Leistungserbringung mit dem geringst möglichen Umfang an Daten auszukommen.

In dieser Hinsicht könnte die Freiwilligkeit der Einwilligung etwa durch folgende Regelung gesichert werden: [421]

Die mangelnde Freiwilligkeit der Einwilligung wird unter anderem vermutet, wenn

1. *eine Leistung der zivilisatorischen Grundversorgung von der Einwilligung der betroffenen Person in die Verarbeitung ihrer Daten abhängig gemacht wird,*
2. *die Einwilligung die Datenverarbeitung in dauerhaften Abhängigkeitsverhältnissen erlauben soll oder*
3. *in einer von der verantwortlichen Stelle vorformulierten Einwilligungserklärung nicht in sachlich trennbare Eigenschaften der Datenverarbeitung eingewilligt werden kann.*

Die Freiwilligkeit der Einwilligung wird vermutet, wenn sie nicht von einer Gegenleistung abhängig gemacht wird.

4) Ausdrückliche und formgerechte Erklärung

Die Einwilligung ist vor der Datenverarbeitung ausdrücklich und präzis sowie in der Form des § 126 BGB zu erteilen. Sollen besonders schützenswerte Daten verarbeitet werden, muss sich, wie in § 4a Abs. 3 BDSG, die Einwilligung ausdrücklich auf diese Daten beziehen.

In seiner künftigen Fassung nach dem Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr erlaubt § 126 Abs. 3 BGB, eine schriftformgebundene Willenserklärung auch in elektronischer Form zu erteilen. Das Datenschutzrecht sollte keine zusätzlichen Formvorschriften schaffen, sondern sich der Formen bedienen, die allgemein für Willenserklärungen vorgesehen sind.

Auf eine gesetzliche Form für die Einwilligung kann nicht verzichtet werden. Der Zweck der bisher allein vorgesehenen Schriftform liegt

- im Schutz der betroffenen Person vor einer übereilten Einwilligung. Sie soll veranlasst werden, sich nicht unbedacht und vorschnell zu äußern.[422] Das schriftliche Vorliegen der

---

[419] S. zur Freiwilligkeit bei Daten für einen verwaltungsrechtlichen Antrag Teil 3 Kap. 3.1.3.

[420] S. Teil 3 Kap. 6.

[421] S. zu Nr. 3 dieser Regelung die Erläuterungen in Teil 3 Kap. 3.3.4.

[422] *Simitis*, in: *ders*. u.a., BDSG, § 4 Rn. 37; *Gundermann*, K&R 2000, 229; *Dörr*, RDV 1992, 167; *Podlech/Pfeiffer*, RDV 1998, 152.

Erklärung soll ihr ermöglichen, ihre Tragweite erkennen zu können.[423] Die vorgeschriebene Form ist eine die Grundrechtsausübung sichernde verfahrensrechtliche Vorkehrung.[424]

- in der Nachvollziehbarkeit der Einwilligung und damit des Umfangs der erlaubten Datenverarbeitung.[425] Art, Umfang und Grenzen der erlaubten Verarbeitung können jederzeit überprüft werden.[426] Dies dient auch der Streitvermeidung.
- in der Sicherstellung eines dauerhaften Beweismittels.[427] Nur mit seiner Hilfe kann die verantwortliche Stelle nachweisen, dass die Einwilligung „ohne jeden Zweifel" (Art. 7 a) DSRL) gegeben worden ist.

Diese Zwecke müssen nach wie vor mit der expliziten Einwilligungserklärung verfolgt werden. Andere Formen der Erklärung als die Schriftform sollten diese Zwecke ebenfalls erfüllen können. Daher wird empfohlen, auch die Äquivalente zur gesetzlichen Schriftform für die Zustimmungserklärung zuzulassen. Die genannten Zwecke können auch mit der elektronischen Form erreicht werden, nicht aber durch ungesicherte elektronische Erklärungen, wie eine einfache E-Mail. Allenfalls dann, wenn bei Inkrafttreten des Gesetzes elektronische Signaturverfahren als Voraussetzung für die elektronische Form noch nicht in ausreichendem Maß verfügbar sein sollten, könnte für einen begrenzten Zeitraum vorübergehend eine elektronische Einwilligung zugelassen, die den unzureichenden Voraussetzungen des § 4 Abs. 2 des Entwurfs für ein novelliertes TDDSG entspricht.[428]

Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich oder elektronisch erklärt werden,[429] so ist – wie nach § 4a Abs. 1 Satz 4 BDSG – die Einwilligungserklärung „im äußeren Erscheinungsbild hervorzuheben".[430]

Die Ausnahmeklausel zum Verzicht auf die vorgeschriebene Form beim Vorliegen besonderer Umstände sollte beibehalten werden. Sie belässt der Form des § 126 BGB den unbedingten Vorrang, vermeidet aber eine allzu starre Regelung, indem sie Ausnahmen zulässt. Wie bisher sollte auf eine abschließende Definition verzichtet werden, wann genau „besondere Umstände" vorliegen. Entscheidend sollen die jeweils spezifischen Verarbeitungsumstände sein. Die Ausnahmemöglichkeit ist allerdings nach allgemeinen Auslegungsgrundsätzen restriktiv anzuwenden.[431] Zur Erhöhung der Rechtssicherheit könnten außerdem gesetzliche

---

423 *Podlech/Pfeiffer*, RDV 1998, 152.

424 *Bizer*, in: Roßnagel, RMD, § 3 TDDSG, Rn. 91; *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 37; *Podlech/Pfeiffer*, RDV 1998, 152; *Bizer* 1992, 145.

425 *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 37.

426 *Bizer*, in: *Roßnagel*, RMD, § 3 TDDSG, Rn. 92.

427 *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 37.

428 S. BT-Drs. 14/6098.

429 Ob eine formularmäßige Einwilligungserklärung nach § 4 Abs. 2 BDSG überhaupt wirksam sein kann, hat der *BGH* bisher – s. *BGHZ* 95, 362 (368) – offengelassen – s. *OLG Naumburg*, VuR 1995, 47.

430 S. näher zu den Anforderungen *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 60a ff.; *Simitis*, in: *ders*. u.a., BDSG, § 4 Rn. 40f.; *Auernhammer*, BDSG, § 4 Rn. 16; *LG Stuttgart*, DuD 1999, 299.

431 *LG Darmstadt*, RDV 1999, 29; *Simitis*, in: *ders*. u.a., BDSG, § 4 Rn. 43.

Beispielsfälle genannt werden, wie große Eilbedürftigkeit der Datenverarbeitung,[432] Unmöglichkeit der Einhaltung der gesetzlichen Form[433] oder drohende Zweckverfehlung.[434]

Zum Schutz von Kindern erscheinen zwei kleinere Regelungen sinnvoll zu sein. Unabhängig davon, ob die datenschutzrechtliche Einwilligung als rechtsgeschäftliche Erklärung nach § 183 BGB[435] oder als tatbestandsausschließende tatsächliche Erklärung verstanden wird,[436] besteht Einigkeit, dass für sie keine Geschäftsfähigkeit erforderlich ist. Auch Jugendliche können die Erklärung abgeben, wenn sie die hierfür erforderliche Einsichtsfähigkeit haben.[437] Für Kinder können die gesetzlichen Vertreter die Einwilligung erklären. Da insbesondere über das Internet vielfach versucht wird, personenbezogene Daten über und durch Minderjährige – zum Teil mit suggestiven Methoden – zu erheben, ist zu ihrem Schutz und zur Gewährleistung von Rechtssicherheit festzulegen, dass für diese bis zum Alter von 14 Jahren sowie für Geschäftsunfähige die Einwilligung des gesetzlichen Vertreters erforderlich ist. Ein schuldhafter Verstoß gegen diese Regelung sollte in den Katalog der Ordnungswidrigkeiten des § 43 BDSG aufgenommen werden.

Das Niederländische Datenschutzgesetz[438] sieht in Art. 5 Abs. 1 eine Regelung zur Zustimmungsfähigkeit Minderjähriger ab dem 16. Lebensjahr vor. Nach dieser muss die Zustimmung zur Datenverarbeitung von den gesetzlichen Vertretern statt von den Minderjährigen erteilt werden. Besondere Regelungen zum Schutz von Kindern sehen auch der Children's Online Privacy Protection Act der USA von 1998[439] und Art. 24 und 25 der Guidelines des Electronic Commerce Promotion Council of Japan (ECOM) vom März 1998[440] vor.

3.3.2 Grenzen der Einwilligung

Zwar ist die Einwilligung ein Ausdruck der informationellen Selbstbestimmung, doch darf diese nicht auf die individuelle Verfügungsmacht beschränkt werden. Vielmehr ist die Doppelfunktion des Rechts auf informationelle Selbstbestimmung zu beachten. Daher sind bei einer Zustimmung auch die Auswirkungen einzelner Akte der Selbstbestimmung auf die ge-

---

[432] Wie z.B. in medizinischen Notfällen– s. z.B. *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 55; *Gola/Schomerus*, BDSG, § 4 Rn. 6.1; *Däubler/Klebe/Wedde*, BDSG, § 4 Rn. 13; *Wohlgemuth* 1992, Rn. 114; *Roßnagel*, NJW 1989, 2304; oder bei dem Wunsch der betroffenen Person nach sofortiger Ausführung eines telefonischen Auftrags – s. z.B. *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 44; allgemein für die Bestellung als andere zulässige Form der Einwilligung s. *Lamberg*, DÖV 1979, 894.

[433] Wenn sich etwa die betroffene Person im Ausland aufhält und die Einwilligung für die Durchführung eines Geschäfts erforderlich ist, an dem die betroffene Person Interesse hat – s. z.B. *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 55; *Däubler/Klebe/Wedde*, BDSG, § 4 Rn. 13; *Roßnagel*, NJW 1989, 2304; *Hollmann*, MedR 1992, 180; oder bei telefonischen Meinungsumfragen– s. *Gola/Schomerus*, BDSG, § 4 Rn. 6.1; *Schulz* 1998, 62.

[434] So z.B. bei Straßeninterviews – s. z.B. *Gola/Schomerus*, BDSG, § 4 Rn. 6.1; *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 55; *Simitis*, in: *ders*. u.a.,, BDSG, § 4 Rn. 54. In der Literatur wird auch der Fall der Geschäftsbeziehung von längerer Dauer genannt, bei der es nicht vertretbar erscheint, bei jeder neuen Datenverarbeitung eine neue schriftliche Einwilligung zu verlangen – s. z.B. *Gola/Schomerus*, BDSG, § 4 Rn. 6.1; *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 55; *Schaffland/Wiltfang*, BDSG, § 4 Rn. 9; *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 44; *Roßnagel*, NJW 1989, 2304.

[435] So z.B. *Simitis*, in: *ders*. u.a. BDSG, § 4 Rn. 28; *Däubler/Klebe/Wedde*, BDSG, § 4 Rn. 9; *Wengert/Widmann/Wengert*, NJW 2000, 1294; *Podlech/Pfeiffer*, RDV 1998, 152; *Kothe*, AcP 85 (1985), 152 ff.

[436] Als „Realhandlung" sehen die Einwilligung z.B. *Gola/Schomerus*, BDSG, § 4 Rn. 5.5; *Dörr/Schmidt*, BDSG, § 4 Rn. 3; *Auernhammer*, BDSG, § 4 Rn. 11; *Uckermann*, DuD 1979, 166.

[437] S. z.B. *Däubler/Klebe/Wedde*, BDSG, § 4 Rn. 10; *Gola/Schomerus*, BDSG, § 4 Rn. 5.5; *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 28;

[438] Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

[439] S. *Grimm/Roßnagel*, DuD 2000, 446 ff.

[440] *ECOM*, Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector (Version 1.0), March 1998, www.ecom.or.jp/ecom_e/guide/personal.pdf.

samte Kommunikationsverfassung der Gesellschaft zu berücksichtigen, die auf die Kommunikations- und Partizipationsfähigkeit des Einzelnen gegründet ist.[441] Hinsichtlich eines Trends, die informationelle Selbstbestimmung auf die Möglichkeit der wirtschaftlichen Verwertung der eigenen Daten zu reduzieren, ist an die Feststellung des Bundesverfassungsgerichts zu erinnern, dass das allgemeine Persönlichkeitsrecht nicht im Interesse der Kommerzialisierung der eigenen Person gewährleistet wird.[442] Wird diese Erkenntnis auf das unveräußerliche Grundrecht auf informationelle Selbstbestimmung übertragen, schließt dies die wirtschaftliche Verwendung personenbezogener Daten nicht aus, verhindert aber deren grenzenlose Kommerzialisierung und fordert Grenzen der Einwilligungsfähigkeit im Allgemeininteresse.

Ein Ausschluss der Einwilligungsmöglichkeit sollte allerdings auf gravierende Gefährdungen der Selbstbestimmung beschränkt bleiben. Ein solcher sollte gelten, wenn das Recht

- bestimmte Verbote zum Schutz der betroffenen Person ausdrücklich festlegt,[443]
- bestimmte Geheimhaltungspflichten ausdrücklich festlegt – gegenüber einer Einschränkung der Geheimhaltungspflicht (z.B. § 35 SGB I), nicht gegenüber der Offenbarung eines bestimmten Datums im Einzelfall,
- bestimmte Regelungsprärogativen festlegt (z.B. für tarifvertragliche und betriebsverfassungsrechtliche Vereinbarungen im Arbeitsrecht),
- bestimmte Zweckbindungen ausdrücklich festlegt und Zweckentfremdungen ausdrücklich verhindert (z.B. Protokolldateien nach § 14 Abs. 4 und § 31 BDSG) – gegenüber der generellen Einschränkung, nicht gegenüber der Offenbarung eines bestimmten Datums im Einzelfall.

Eine Regelung, die diese Grenzen festlegt, könnte etwa lauten:

Eine Einwilligung erlaubt eine Datenverarbeitung nicht, soweit eine Rechtsvorschrift

1. *die Datenverarbeitung zum Schutz der betroffenen Person ausdrücklich verbietet,*
2. *die Entscheidung über die Zulässigkeit der Datenverarbeitung einem anderen Entscheidungsträger überträgt oder*
3. *eine bestimmte Zweckbindung oder Geheimhaltungspflicht ausdrücklich festlegt.*

3.3.3 Formulareinwilligung

Einwilligungsformulare sind in Massenverfahren unvermeidlich. In ihnen muss die verantwortliche Stelle mit Modellklauseln arbeiten, eine individuelle Aushandlung von Einwilligungserklärungen ist in diesen Fällen nicht praktikabel.

Für Einwilligungserklärungen in Allgemeinen Geschäftsbedingungen gilt nach § 3 AGBG, dass sie keine versteckten oder überraschenden Klauseln enthalten dürfen, und nach § 9 AGBG, dass sie sich an dem Leitbild des BDSG orientieren müssen. Danach dürfen die Erklärungen, die sich auf alle Phasen der Datenverarbeitung beziehen können, nicht unausgewogen sein, nicht von der Einhaltung bestimmter Schweigepflichten oder Berufsgeheimnisse

---

441 *Simitis*, DuD 2000, 721: „Je deutlicher ein systematischer, formal durch das Einverständnis der betroffenen Personen durchaus abgedeckter Verkauf der eigenen Daten die informationelle Selbstbestimmung unterläuft, damit aber auch die Kommunikations- und Partizipationsfähigkeit der betroffenen Personen mehr und mehr zur Fiktion erstarren lässt, desto nachhaltiger wird die Schutzpflicht des Staates aktiviert."

442 *BVerfGE* 101, 361 (385).

443 Z.B. bei einem Verbot von Genomanalysen gegenüber Versicherungen, wie es der Bundesrat im November 2000 gefordert hat – s. BR-Drs. 530/00; s. hierzu auch *Fisahn*, ZPR 2001, 49 ff.; Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13.10.2000.

befreien,[444] keine zu weitgehenden Eingriffe in die informationelle Selbstbestimmung ermöglichen und nicht von gesetzlichen Beschränkungen oder Interessenabwägungen befreien. Ansonsten werden sie von der Rechtsprechung für unwirksam erklärt.[445]

Diese Regelungen beseitigen aber nicht alle Probleme von Formulareinwilligungen. In der Regel hat derjenige, der die Formulare vorlegt, eine solche Vormachtstellung, dass er auch den Inhalt der Einwilligung allein bestimmt.[446] Um die Freiwilligkeit der Einwilligung zu sichern, muss das Datenschutzrecht verhindern, dass Marktmacht Einwilligungen faktisch erzwingt, weil sie keine Alternative zulässt.[447]

Von Formularverträgen sollte daher gefordert werden, dass sie „einwilligungsfreundlich" ausgestaltet werden. Denn bei dem Problem der freiwilligen Einwilligung in Formularverträge geht es nur um Verarbeitungszwecke, die jenseits des Vertrags liegen, wie zum Beispiel die Datenverarbeitung zu Zwecken des Marketing, der Werbung, der Kundenpflege oder der Wartung. In diesen Fällen können alle unterschiedlichen Datenkategorien, Zwecke, Verarbeitungsalternativen oder Empfänger (Empfängerkategorien) jeweils getrennt dargestellt werden (etwa mit Kästchen zum Ankreuzen), so dass die betroffene Person es sich aussuchen kann, welcher Datenverarbeitung sie zustimmen will und welcher nicht. Verknüpfungen zwischen den Einwilligungsgegenständen sollten nur zulässig sein, wenn sie für den Verarbeitungszweck erforderlich sind. In diesem Zusammenhang kann auch darauf hingewiesen werden, wenn die Verweigerung einer Zustimmung mit tatsächlichen Folgen verbunden ist. Eigentlich wird diese Gestaltung des Formulars bereits vom Kopplungsverbot[448] gefordert. Fehlt eine mögliche „einwilligungsfreundliche" Gestaltung, sollte die das Gesetz vermuten, dass die Freiwilligkeit der Einwilligung fehlt.

Die Gestaltung der Einwilligungsformulare sollte Gegenstand der Selbstregulierung sein und nach den in Teil 3 Kap. 4 beschriebenen Verfahren beschlossen und genehmigt werden. Damit einher geht eine aufsichtsbehördliche Präventivkontrolle,[449] in der auch geprüft werden kann, ob für Leistungen der zivilisatorischen Grundversorgung Alternativen ohne zusätzliche Datenverarbeitung angeboten werden.[450]

Darüber hinaus unterliegt die Verwendung der Einwilligungsformulare der (erweiterten) gesellschaftlichen Kontrolle durch Verbandsklagen nach dem AGB und durch Verbands- und Konkurrentenklagen nach dem UWG.[451]

3.4 Erforderlichkeit der Verarbeitung personenbezogener Daten

Wenn die Verarbeitung personenbezogener Daten ein Eingriff in das Recht auf informationelle Selbstbestimmung ist,[452] darf sie nur im jeweils erforderlichen Umfang erfolgen.[453] Dies

---

444 *OLG Schleswig*, DSB 2/98, 15; *LG Bonn*, RDV 1995, 246; *Gola*, DSB 10/99, 8.

445 S. z.B. *BGHZ* 95, 362 (367f.); *OLG Düsseldorf*, VuR 1995, 353; *OLG Frankfurt*, DuD 1999, 232f.; *LG Halle*, CR 1998, 86; *Gola*, DSB 10/99, 9, *Kothe*, AcP 85 (1985), 134f.

446 *Schrader* 1999, 2.

447 S. hierzu näher *Bergmann/Möhrle/Herb*, § 4 Rn. 34; *Schapper/Dauer*, RDV 1987, 170 m.w.N.*; Schapper/Dauer*, CR 1987, 497; *Schmidt*, JZ 1974, 245.

448 S. Teil 3 Kap. 3.3.1.

449 Eine aufsichtsbehördliche Präventivkontrolle ist beispielsweise auch in der Versicherungswirtschaft vom Bundesamt für das Versicherungswesen praktiziert worden. Die genehmigte Klausel ist abgedruckt in Veröffentlichungen des Bundesaufsichtsamtes für das Versicherungswesen 1979, 408; dazu *Simitis*, in: *ders. u.a.*, BDSG, § 4 Rn. 21 m.w.N.

450 S. Teil 3 Kap. 3.3.1.

451 S. Teil 3 Kap. 9.3.

452 S. Teil 2 Kap. 4.1.1.

453 *BVerfGE* 65, 1 (43, 46).

gilt aus verfassungsrechtlichen Gründen auch für den Schutz der informationellen Selbstbestimmung im nicht öffentlichen Bereich. Der Erforderlichkeitsgrundsatz bezieht sich nach Art. 7 b) bis f) DSRL auf alle Erlaubnistatbestände der Datenverarbeitung ohne Einwilligung der betroffenen Person, also auch auf jede Datenverarbeitung im nicht öffentlichen Bereich.

Diese Anforderung gilt uneingeschränkt für die Verarbeitung mit gezieltem Personenbezug. Für die Verarbeitung ohne gezielten Personenbezug ist sie dahingehend zu spezifizieren, dass alle für den spezifischen Zweck (Kommunikationsdienstleistung, Suche) nicht erforderlichen Daten vermieden und die Daten nach Zweckerfüllung sofort gelöscht werden.[454]

3.4.1 Erforderlichkeit als Begrenzung der Datenverarbeitung

Das Erforderlichkeitsprinzip beschreibt eine normative Zweck-Mittel-Relation. Wie das Bundesverfassungsgericht festgestellt hat, müssen sich

> „alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Ziels erforderliche Minimum beschränken".[455]

Der Zweck der Datenverarbeitung ergibt sich aus ihrer Legitimation, aus der Einwilligung, aus dem Vertrag, dem vertragsähnlichen Vertrauensverhältnis, dem Antrag oder einer der anderen genannten gesetzlichen Erlaubnisse. Er ist bei der Inanspruchnahme eines Erlaubnistatbestands zur unfreiwilligen Datenverarbeitung von der verantwortlichen Stelle zu präzisieren.

Erforderlich ist die Datenverarbeitung, wenn auf sie zum Erreichen des Zwecks nicht verzichtet werden kann, wenn also die aus dem Zweck sich ergebende Aufgabe der verantwortlichen Stelle ohne die Datenverarbeitung nicht, nicht rechtzeitig, nicht vollständig oder nur mit unverhältnismäßigem Aufwand erfüllt werden kann.[456] Das personenbezogene Datum muss bezogen auf das Ob, die Zeitgerechtigkeit, die geforderte Qualität und die Wirtschaftlichkeit der Aufgabenerfüllung „conditio sine qua non" sein. Die bloße Eignung oder Zweckmäßigkeit eines Datums zur Aufgabenerfüllung allein begründet keinesfalls die Erforderlichkeit. Die Geeignetheit ist zwar notwendige, nicht aber hinreichende Bedingung der Erfüllung des Erforderlichkeitsbegriffs.[457] Arbeitserleichterungen oder Ersparnisse im Blick auf künftig vielleicht nötig werdende Zusatzaufwendungen allein reichen als Grundlage für eine zulässige Datenverarbeitung nicht aus.

Das Erforderlichkeitsprinzip führt zu folgenden Begrenzungen einer an sich zulässigen Datenverarbeitung:

(1) Es dürfen die *Daten* verarbeitet werden, die für das Erreichen des Zwecks unabdingbar sind. Dies bedeutet, dass eine Datenverarbeitung auf Vorrat nicht erlaubt ist.[458] Eine vorsorgliche Datenverarbeitung für künftige Zwecke ist ebenso unzulässig wie die Verarbeitung von üblicherweise benötigten Daten, die im Einzelfall jedoch nicht erforderlich sind.[459]

(2) Die *Datenverarbeitung* ist auf die für das Erreichen des Zwecks notwendigen Phasen zu beschränken. Beispielsweise ist eine Speicherung der Daten dann zulässig, wenn eine Erhebung der Daten nicht ausreicht, eine Übermittlung dann erlaubt, wenn die Kenntnisnahme des Dritten unverzichtbar ist.

---

454 S. Teil 3 Kap. 2.6.

455 *BVerfGE* 65, 1 (46).

456 In Übernahme einer von *Podlech* entwickelten Formulierung, h.M., ähnlich auch beispielsweise *Dammann*, in: *Simitis u.a.*, BDSG, § 14 Rn. 15.

457 S. *Globig*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.7 Rn. 58.

458 S. hierzu auch Teil 3 Kap. 3.5.

459 S. *BVerfGE* 65, 1 (46); s. ferner ; *Geiger*, in: *Simitis u.a.*, BDSG, § 13 Rn. 26 m.w.N.; *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 37.

(3) Die Datenverarbeitung darf in dem *Zeitraum* erfolgen, in dem sie zur Zweckerreichung notwendig ist. Nach Art. 6 Abs. 1 e) DSRL sollen die Daten nicht länger in einer Form aufbewahrt werden, die eine Identifizierung der betroffenen Person ermöglicht, als dies für die Realisierung der Zwecke erforderlich ist, für die sie erhoben oder verarbeitet werden.[460] Dies erfordert die frühestmögliche Löschung der Daten.[461] Erfordern gesetzliche Vorschriften die Aufbewahrung der Daten zu anderen Zwecken, sind die Daten zu anonymisieren oder, wenn der Personenbezug herstellbar sein muss, zu pseudonymisieren.[462] Sofern dies im Einzelfall erforderlich ist, kann der Personenbezug wieder hergestellt werden.

Die Forderung, die Datenverarbeitung auf den erforderlichen Zeitrahmen zu beschränken, sollte durch konkrete Prüf- und Löschungspflichten unterstützt werden. Allerdings hängt die Bestimmung einer Frist, innerhalb derer zu prüfen ist, ob die Daten gelöscht werden können, von den spezifischen Aufgaben der verantwortlichen Stelle ab. Konkrete Fristen können daher nur bereichsspezifisch bestimmt werden. Ähnliches gilt für Löschungsfristen. Für sie kommt hinzu, dass einer Löschung nicht mehr erforderlicher Daten in vielen Verwendungszusammenhängen spezifische Aufbewahrungspflichten entgegenstehen. Prüf- und Löschungsfristen sollten daher, soweit eine gesetzliche Regelung als hilfreich erscheint, in bereichsspezifischen Regelungen festgelegt werden. Im Rahmen der allgemeinen Regelungen des BDSG sollte die Festlegung von Prüf- und Löschungsfristen und deren Durchsetzung Aufgabe des Datenschutzmanagementsystems sein.[463]

Für die Löschung personenbezogener Daten ist es unzureichend, sie lediglich als gelöscht zu kennzeichnen, vielmehr müssen sie tatsächlich physisch gelöscht werden. Gibt es vom zu löschenden Datum mehrere Kopien, so ist diese physische Löschung auf alle Kopien zu erstrecken. Insbesondere bei der Datenverarbeitung ohne gezielten Personenbezug muss darauf geachtet werden, dass, sofern überhaupt eine Protokollierung stattfindet, die Protokolle in den Löschungsprozess der Primärdaten einbezogen werden.

Daten gelten als gelöscht, wenn sie mit der heute verfügbaren sowie für die für die Daten relevanten Zeiträume zu erwartenden Technik mit vertretbaren Kosten nicht wiederhergestellt werden können. Diese bedeutet derzeit beispielsweise, dass zu löschende Daten auf magnetischen Festplattenspeichern mindestens zehn mal mit Zufallsmustern überschrieben werden müssen.[464] Ist wegen des besonderen Werts der zu löschenden Daten mit einem Ausbau der Festplatte und ihrem Lesen in einem Spezialgerät zu rechnen, dann ist ein mehrhundertfaches Überschreiben mit Zufallsmustern oder gar die chemische Auflösung des Datenträgers geboten, bevor er die verantwortliche Stelle verlässt. In vielen Fällen wird eine Zerstörung des Datenträgers (Zerhacken, Schreddern, Verbrennen, Entmagnetisieren) erforderlich sein.[465] Bei nicht-automatisierten Dateien und Akten ist das Schwärzen der Schriftzeichen oder die physische Vernichtung erforderlich.[466]

---

460 *BVerfGE* 65, 1 (51).

461 *BVerfGE* 100, 313 (362). Statt Löschung können die Daten auch mit einem Verwertungsverbot belegt werden. Zu prüfen ist, ob ihre Aufbewahrung für den Rechtsschutz der betroffenen Person nicht notwendig ist – *BVerfGE* 100, 313 (364f.).

462 S. sogleich unter (4).

463 S. hierzu Teil 3 Kap. 4.1.

464 S. hierzu auch *Der Berliner Datenschutzbeauftragte*, Jahresbericht 1988, Anlage 8 „Informationen zur Datenträgervernichtung", Abgeordnetenhaus, Drs. 10/2652, 41f.; *Heymann*, CR 1992, 370; *Innenministerium BW*, Hinweis Nr. 31 zur Vernichtung von Datenträgern, CR 1993, 496 ff. Einen Anhaltspunkt bieten auch die DIN-Normen 32 757 und 33 858 über die Vernichtung von Informationsträgern.

465 S. hierzu *Schild*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.3, Rn. 83.

466 *Demke/Schild*, § 10 Erl. III.; 17. TB des Hess. LfD, 138 ff., LT-Drs. 12/4040, 69 ff.

(4) Ein *Personenbezug* darf nur in dem Umfang hergestellt oder aufrecht erhalten werden, in dem er für das Erreichen des Zwecks unverzichtbar ist. Auch diese Begrenzung ergibt sich aus Art. 6 Abs. 1 e) DSRL. Sie hat zwei Ausprägungen. Zum Einen sind Daten im Verarbeitungsprozess so früh wie möglich zu anonymisieren oder zu pseudonymisieren, um so bald wie möglich ihren Personenbezug zu verlieren.[467] Zum Anderen sind Daten, soweit dies für die Zweckerfüllung möglich ist, von Anfang an in anonymer oder pseudonymer Form zu verarbeiten.[468]

Diese Anforderungen des Erforderlichkeitsprinzips könnten etwa in folgender Vorschrift geregelt werden:

(1) Die verantwortliche Stelle verarbeitet personenbezogene Daten nur in dem Umfang, in den Formen und in den Zeiträumen, die für das Erreichen des zulässigen Zwecks erforderlich sind.

(2) Die Verarbeitung personenbezogener Daten ist nicht erforderlich, wenn die verantwortliche Stelle für das Erreichen des zulässigen Zwecks

1. *auf die personenbezogenen Daten verzichten kann,*
2. *anonyme oder pseudonyme Daten verarbeiten kann,*
3. *die verarbeiteten Daten löschen, anonymisieren oder pseudonymisieren kann.*

(3) Die Begrenzung der Datenverarbeitung auf das Erforderliche wird soweit möglich durch das genutzte Datenverarbeitungssystem und die Organisation des Verfahrens gewährleistet.

Die Beseitigung des Personenbezugs kann im öffentlichen Bereich auch Voraussetzung für die Wahrnehmung von Informationsfreiheiten sein.[469] Die bestehenden und geplanten Informationszugangsgesetze ermöglichen den Zugang zu personenbezogenen Daten nur unter engen Voraussetzungen und unter Abwägung der konkurrierenden Interessen. Da viele öffentliche Informationssysteme personenbezogene Daten verarbeiten, dürfte der Personenbezug vielfach den Informationszugang ausschließen. Eine Anonymisierung oder Pseudonymisierung der Daten ist somit auch notwendig, um den Vollzug dieser Regelungen zu gewährleisten.

Eine frühzeitige Beseitigung des Personenbezugs ist außerdem notwendig, um zu verhindern, dass personenbezogene „integrierte Informationssysteme“[470] aufgebaut werden, aus denen sich zusammen mit anderen Datenbeständen Profile zusammenfügen lassen.[471] Dieses Risiko wird künftig zunehmen, weil immer leistungsfähigere Data-Mining-Techniken und andere Suchverfahren entwickelt werden, die auch in verteilten Datenbeständen, die zur Profilbildung gewünschten Daten zusammen führen können. Eine vorausgehende Datenverarbeitung auf Vorrat – etwa in einem Data Warehouse – ist hierfür nicht mehr notwendig. Die Profile können aus den operativen Daten gewonnen werden. Je fortgeschrittener solche Verfahren sind, um so mehr muss darauf geachtet werden, möglichst früh die Daten zu löschen oder zumindest ihren Personenbezug zu vermeiden.[472]

---

467 S. hierzu auch *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 75.

468 S. die folgenden Kap. 3.4.2 und 3.4.3.

469 S. hierzu auch *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 75

470 *BVerfGE* 65, 1 (42).

471 S. hierzu auch *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 75

472 S. Entschließung: Data Warehouse, Data Mining und Datenschutz der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15. März 2000, http://www.bfd.bund.de/information/DS-Konferenzen/59dsk_ent2.html, sowie 21. Tätigkeitsbericht des LfD Schleswig-Holstein, 1999, Tz. 7.3, http://www.datenschutzzentrum.de/material/tb/tb21/kap7.htm#Tz7.3.

Das schweizerische Bundesgesetz über den Datenschutz[473] fordert in Art. 21 von öffentlichen Stellen, personenbezogene Daten, die sie nicht mehr benötigen, zu anonymisieren oder zu löschen, soweit sie nicht mehr für Beweis- oder Sicherungszwecke benötigt werden oder an das Bundesarchiv abzuliefern.

3.4.2 Vermeidung des Personenbezugs als Gestaltungsprinzip

Das Erforderlichkeitsprinzip bezieht sich auf einen gegebenen Zweck, ein gegebenes technisches System und einen gegebenen Datenverarbeitungsprozess. Für diese vorgegebenen Umstände veranlasst es die Frage, ob eine konkrete Datenverarbeitung erforderlich ist. Das Erforderlichkeitsprinzip verpflichtet nicht, das unter bestimmten Umständen Erforderliche selbst noch einmal durch Überprüfung der Umstände am Erforderlichkeitsprinzip zu messen und nach diesem die Umstände zu ändern.

Das Gestaltungsprinzip der Vermeidung des Personenbezugs, das in § 3 Abs. 4 TDDSG und § 12 Abs. 5 MDStV erstmals geregelt und in § 3a BDSG in abgeschwächter Form übernommen wurde, entspringt zwar auch der grundrechtlich motivierten Erforderlichkeitsprüfung, geht aber weit über das herkömmliche Erforderlichkeitsprinzip des Datenschutzrechts hinaus. Denn es verlangt von der verantwortlichen Stelle eine aktive Gestaltung ihrer technisch-organisatorischen Verfahren in der Form, dass diese möglichst keine oder so wenig personenbezogene Daten wie möglich verarbeitet. Es verlangt von ihr sogar, ihre Zwecke im Sinn einer „datensparsamen“ Konkretisierung zu überdenken: Verarbeitungszwecke können auf unterschiedlichen Ebenen konkretisiert werden. So kann etwa der Zweck, Bilder, Filme, Musik oder Datenübertragungsleistungen abzurechnen, in unterschiedlichen Abrechnungsformen erfolgen. Wenn eine gewählte Abrechnungsform als Zweck der Erforderlichkeitsprüfung zugrunde gelegt wird, kann die Verarbeitung personenbezogener Daten erforderlich sein. Wird der abstraktere Zweck, die erbrachte Leistung abzurechnen, zum Bezugspunkt der Erforderlichkeitsprüfung, ergibt sich für die verantwortliche Stelle die Pflicht, nach einer Gestaltung der Abrechnungsverfahren zu suchen, die diesen Zweck erfüllt, aber ohne die Verarbeitung personenbezogener Daten auskommt. Eine solche Systemgestaltung ist der Kern des Systemdatenschutzes.[474]

Das Ziel, den Personenbezug zu vermeiden, ist dreistufig zu sehen, nicht nur einstufig wie in § 3 Abs. 4 TDDSG, § 12 Abs. 5 MDStV und § 3a BDSG:

- Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass sie ohne personenbezogene Daten durchgeführt werden können.
- Ist dies nicht möglich, ist der Datenverarbeitungsprozess so zu organisieren und sind die Datenverarbeitungssysteme so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten minimiert wird, indem weitgehend auf einen Personenbezug verzichtet wird.
- Sofern dies nicht möglich ist, ist der Datenverarbeitungsprozess so zu organisieren und sind die Datenverarbeitungssysteme so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten zeitlich möglichst kurz gehalten wird und die personenbezogenen Daten frühestmöglich gelöscht, anonymisiert oder pseudonymisiert werden.

Produkte, für die zertifiziert ist, dass sie diese Ziele erfüllen, sollten vorrangig verwendet werden.[475]

---

[473] Gesetz vom 19.6.1992 (Stand. 7.7.1998).

[474] S. Teil 2 Kap. 2.1.

[475] S. hierzu Teil 4.3.3.

Um das Verhältnis zwischen der Erforderlichkeit als Begrenzung der Datenverarbeitung und der Erforderlichkeit als Gestaltungsprinzip klar zu stellen: Die mögliche Vermeidung des Personenbezugs ist zweimal zu prüfen.

Erstens ist zu prüfen, ob die Daten unter den gegebenen Umständen (Zwecke, Verarbeitungsprozess) erforderlich sind. Ist dies nicht der Fall, so ist die zwingende Folgerung, dass der Personenbezug zu vermeiden und notfalls die Datenverarbeitung zu unterlassen ist.[476]

Zweitens ist zu prüfen, ob die gegebenen oder geplanten Umstände der Datenverarbeitung so verändert werden können, dass der Personenbezug nicht mehr erforderlich ist. Kann im Prinzip auf den Personenbezug verzichtet werden, entsteht daraus eine Rechtspflicht, die Verfahren und Systeme „datensparsam" zu gestalten, wenn dies technisch möglich und verhältnismäßig ist.

Die Anforderung einer „datensparsamen" Systemgestaltung sollte wie in den bisherigen Regelungen als Optimierungsanforderung und nicht als Verarbeitungsvoraussetzung ausgestaltet werden. Hierfür sprechen drei Gründe: Zum Einen ist aus verfassungsrechtlichen Gründen, die grundsätzliche Entscheidungsautonomie der verantwortlichen Stelle für die Organisation ihrer Verarbeitungsprozesse zu respektieren. Zum anderen unterliegt die Gestaltungsanforderung dem Vorbehalt des technisch Möglichen und der Verhältnismäßigkeit. Schließlich würde die Ausgestaltung der Anforderung als Verarbeitungsvoraussetzung jede Datenverarbeitung mit einer nicht tragbaren Rechtsunsicherheit belasten. Da eine über die Mindestanforderung[477] hinausgehende Optimierung der Prozesse und Systeme verlangt wird, kann immer darüber gestritten werden, ob nicht eine noch bessere Verwirklichung des Vermeidungsziels möglich wäre. Hiervon sollten sowohl die verantwortlichen Stellen als auch die Kontrollstellen entlastet werden.

Die Umsetzung des Vermeidungsziels sollte vor allem durch ein Datenschutzmanagementsystem und durch den Wettbewerbsmechanismus eines gesetzlichen Datenschutzaudits, sekundär durch Anforderungen der Kontrollstellen erreicht werden. Die verantwortliche Stelle sollte in ihrem Datenschutzkonzept nachweisen, dass sie das Gestaltungsziel erreicht hat.[478] Die Optimierung der Verarbeitungsprozesse und -systeme ist ein zentraler Maßstab für die Honorierung der Datenschutzanstrengungen durch ein Datenschutzauditzeichen. Ihr Fortschritt ist im Rahmen des Auditverfahrens zu belegen und zu überprüfen.[479] Eindeutige Verstöße gegen die Gestaltungsanforderung können schließlich von den Kontrollstellen beanstandet und ihre Beseitigung durchgesetzt werden.

3.4.3 Pflicht zur Verarbeitung anonymer und pseudonymer Daten

Ein für die künftige Datenverarbeitung besonders bedeutsames Mittel zur Vermeidung des Personenbezugs wird die Verarbeitung anonymer und pseudonymer Daten sein.[480] Insbesondere die Nutzung von Pseudonymen ist gerade für Transaktionen in Netzen der gebotene

---

476 S. hierzu Teil 3 Kap. 3.4.1.

477 Bei den gegebenen Umständen.

478 S. Teil 3 Kap. 4.1.

479 S. Teil 3 Kap 4.2.

480 Zur Forderung nach Anonymität und Pseudonymität s. z.B. *Registratiekamer/Information & Privacy Commissioner* 1995; *Rat für Forschung, Technologie und Innovation* 1995, 2.5, Empfehlung 23; *Art. 29 – Datenschutzarbeitsgruppe*, Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet, www.datenschutz-berlin.de/doc/eu/gruppe29/bbmem_de. htm; *Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft"*, BT-Drs. 13/11002, 94 f; *Simitis* 1997, 285 ff.; *Vogt/Tauss* 1998, Nr. 12.

Kompromiss zwischen dem Bedarf an Authentifizierung der Kooperationspartner und dem Bedarf an Sicherung der informationellen Selbstbestimmung.[481]

Anonyme Daten weisen keinen Personenbezug auf.[482] Denn *Anonymität* ist dadurch gekennzeichnet, dass für Einzelangaben zu einer Person die Wahrscheinlichkeit, dass diese der Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet.[483] Für die Bestimmung der Wahrscheinlichkeit sind das für die verantwortliche Stelle vorhandene oder erwerbbare Zusatzwissen, die gegenwärtigen und künftigen technischen Möglichkeiten der elektronischen Datenverarbeitung, der mögliche Aufwand und die verfügbare Zeit zu berücksichtigen.[484] Praktisch ausgeschlossen erscheint die Aufdeckbarkeit des Personenbezugs, wenn die Anonymitätsmenge, die durch die bekannten Merkmale der betroffenen Person eingegrenzt werden kann, ausreichend groß ist und die Wahrscheinlichkeiten, die betroffene Person zu sein, in ihr ausreichend gleichmäßig verteilt sind. Anonymität ist wie Personenbeziehbarkeit relativ zu der jeweiligen verantwortlichen Stelle zu bestimmen, für die Möglichkeit, den Personenbezug aufdecken und herstellen zu können, aufgrund der Umstände unterschiedlich wahrscheinlich sein kann.[485]

Pseudonymität ist gegeben, wenn die betroffene Person ein Kennzeichen benutzt, durch das die Wahrscheinlichkeit, dass Daten der Person zugeordnet werden können, so gering ist, dass sie ohne Kenntnis der jeweiligen Zuordnungsregel zwischen Kennzeichen und Person nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet. Neben aktiv benutzten Pseudonymen, die sich die betroffene Person selbst auswählt, um mit ihrer Hilfe ihre informationelle Selbstbestimmung zu schützen,[486] gibt es auch Pseudonyme, die von Dritten ohne Zutun der betroffenen Person vergeben werden[487] und ihr entweder bekannt[488] oder unbekannt[489] sind. Während bei Anonymität niemand – auch nicht die betroffene Person – den Bezug eines Merkmals zu einer bestimmten Person herstellen kann, gibt es bei Pseudonymität eine Regel (oder Liste), über die eine solche Zuordnung möglich ist. Bei Pseudonymität ist daher zwischen den Personen, die die Zuordnungsregel kennen und denen, die sie nicht kennen, zu unterscheiden. Pseudonyme Daten sind für den Kenner der Zuordnungsregel personenbeziehbar, für alle anderen sind sie anonyme Daten.[490] Für diese anderen verantwortlichen Stellen ist auf die gleichen Merkmale abzustellen wie für anonyme

---

481 S. hierzu Teil 3 Kap. 5.1; s. auch z.B. *Roßnagel* 1994, 245f.; *ders*., in: *ders*., RMD, Einführung, Rn. 61f.; *provet/GMD*, 210 ff.; *Bizer*, in: *Roßnagel*, RMD, § 3 TDDSG, Rn. 175 ff.; *Roßnagel/Scholz*, MMR 2001, 721f.

482 Dies gilt für alle Daten, die nicht mit vertretbarem Aufwand einer konkreten Person zugeordnet werden können – sei es, dass die Daten in dieser Weise aggregiert sind oder dass es für sie keine Zuordnungsregel gibt.

483 S. *Dammann*, in: *Simitis u.a.*, BDSG, § 3 Rn. 202 ff.; *Gola/Schomerus*, BDSG, § 3 Anm. 14.2; *Roßnagel/Scholz*, MMR 2000, 723. Bereits im Volkszählungsurteil, *BVerfGE* 65, 1 (49, 68), verweist das *BVerfG* im Zusammenhang mit den notwendigen Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts auf das Gebot einer möglichst frühzeitigen (faktischen) Anonymisierung, ohne diesen Begriff allerdings näher zu erläutern. In späteren Entscheidungen betont das Gericht ausdrücklich, dass von „Verfassungs wegen lediglich eine faktische Anonymität" gefordert sei – s. *BVerfG*, NJW 1987, 2805 (2807); NJW 1988, 962 (963). Zur „ausreichenden" Anonymisierung auf Grund allgemeiner Erfahrung s. auch *Hammerbacher*, DuD 1984, 187.

484 *Möncke*, DuD 1998, 565; *Tinnefeld/Ehmann* 1998, 187; *Roßnagel/Scholz*, MMR 2000, 723f.; *BVerfG*, NJW 1987, 2805 (2807).

485 S. *Roßnagel/Scholz*, MMR 2000, 721 ff.

486 Diese Pseudonyme sind in §§ 5 Abs. 2 und 7 Abs. 1 Nr. 1 SigG geregelt.

487 Stichwort: „Anonymous (=Pseudonymous) Profiling" – *Schaar*, DuD 2001, 384f.

488 Z.B. durch angemeldete Cookies – s. hierzu z.B. *Schaar*, DuD 2001, 384.

489 S. zu einem Internetwerbeverfahren z.B. *Hillenbrand-Beck/Gress*, DuD 2001, 389. Ein anderes Beispiel sind Pseudonymisierung z.B. in der medizinischen Forschung.

490 Ebenso Begründung zu § 22 Abs. 2 LDSG SH., LT-Drs. 14/1738, 66f.

lichen Stellen ist auf die gleichen Merkmale abzustellen wie für anonyme Daten. Für sie haben pseudonyme Daten somit auch keinen Personenbezug.[491]

Pseudonyme haben drei spezifische Eigenschaften, die sie in manchen Zusammenhängen gegenüber vollständiger Anonymität geeigneter erscheinen lassen:

- Daten zu demselben Pseudonym lassen sich miteinander verketten. So können Datensammlungen bis hin zu umfassenden Profilen unter einem Pseudonym entstehen. Dies kann im Interesse des Trägers liegen, weil er trotz fehlender Identifizierung wiedererkannt werden will, etwa um Erleichterungen bei der Registrierung zu haben, um einen Kreditrahmen in Anspruch nehmen zu können oder um Rabatte oder Bonuspunkte zu erhalten.
- Unter Pseudonym können Rechte und Befugnisse geltend gemacht werden, ohne die Identität aufdecken zu müssen. Vollmachten, Berufszulassungen, Amtseigenschaften sowie sonstige Berechtigungen können in einem Attributzertifikat bestätigt werden.[492]
- Die Zuordnungsregel ermöglicht eine Aufdeckung des Pseudonyms. Verfügt ein (vertrauenswürdiger) Dritter über die Zuordnungsregel, besteht gegenüber pseudonym Handelnden die Möglichkeit, sie zur Verantwortung zu ziehen, wenn sie etwa ihre Vertragspflichten nicht erfüllen oder ihre Berechtigungen überschreiten.[493]

Das Konzept pseudonymen Handelns vermag den Zielkonflikt zwischen notwendiger Identifizierung[494] der betroffenen Person und ihrem Wunsch nach Anonymität zu vermeiden, indem es zwischen Regelfall (keine Identifizierung) und Ausnahmefall (Identifizierungsmöglichkeit) unterscheidet. Bei richtiger Handhabung können sich Pseudonyme als ein wichtiges Instrument zur Vermeidung unerfreulicher Konfliktlagen erweisen, bei denen in der Vergangenheit öfter wichtige andere Interessen wie Forschung, Planung, Statistik, Marketing oder Öffentlichkeitsarbeit gegen den Datenschutz ins Feld geführt wurden und umgekehrt.[495]

Die größte Sicherheit gegen die Herstellung eines Personenbezugs bietet *anonymes Handeln*, weil niemand einen Bezug zwischen der Identität des Handelnden und den zu diesem Handeln verarbeiteten Daten kennt.[496]

Bei Pseudonymen kennt definitionsgemäß jemand diesen Bezug.[497] Sie bieten hinsichtlich des Aufdeckungsrisikos durch die Zuordnungsregel unterschiedliche Sicherheit, je nachdem, ob sie nur *selbstaufdeckbare Pseudonyme* sind,[498] für die nur der Pseudonymträger die Zuordnung kennt,[499] oder *durch Dritte aufdeckbare Pseudonyme* sind, bei denen eine dritte Stelle die Zuordnungsregel kennt. Diese sind wiederum danach zu unterscheiden, ob sie von einem

---

491 S. *Roßnagel/Scholz*, MMR 2000, 721 ff.; a.A. für bestimmte Pseudonyme *Schaar*, DuD 2000, 276; *Hillenbrand-Beck/Greß*, DuD 2001, 391.

492 S. zu Pseudonymen mit qualifizierendem Zertifikat *Roßnagel*, in: *ders*., RMD, § 7 SigG, Rn. 62f.; *provet/GMD* 1994, 213 ff.; *Pordesch* 1999, 156 ff.

493 S. hierzu näher unter Teil 3 Kap. 5.2.

494 S. zu Missbrauchsmöglichkeiten von Anonymität *Caronni*, DuD 1998, 623 ff.

495 S. Begründung zu § 10 Abs. 6 und § 22 LDSG SH., LT-Drs. 14/1738, 55f., 67f.

496 Zur datenschutzrechtlichen Bedeutung von Anonymität s. z.B. *Simitis* 1997, 309; zu Anonymitätstechniken s. *Borking*, DuD 1996, 654.; *Arbeitskreis Technik*, DuD 1997, 709 ff.; *Federrath/Pfitzmann*, DuD 1998, 628 ff.; *Demuth/Rieke*, DuD 1998, 623 ff.; *Roessler*, DuD 1998, 619 ff.

497 S. zur Definition im Text oben.

498 Ein vom Nutzer selbst vergebenes Pseudonym ist beispielsweise die frei gewählte Benutzer-ID, die vor der Inanspruchnahme eines Internet-Angebots angegeben werden muss.

499 Der *AK Technik*, DuD 1997, 711 spricht von selbstgenerierten Pseudonymen; s. auch *Roßnagel/Scholz*, DuD 2001, 725.

vertrauenswürdigen Dritten vergeben werden, der allein über die Zuordnungsregel verfügt,[500] oder vom ersten *Datenverwender*, der im Unterschied zum vertrauenswürdigen Dritten ein eigenes Verarbeitungsinteresse hat und trotz Pseudonym die Daten personenbezogen verwenden kann.[501]

Für alle Ausprägungen der von der betroffenen Person selbstgewählten Pseudonyme gilt, dass mit Hilfe von Zertifikaten unter Pseudonym auch digital signiert werden kann (*digitale Pseudonyme*). Das Signaturgesetz sieht jedoch nur durch einen Zertifizierungsdiensteanbieter mit einem digitalen Zertifikat versehene und damit durch ihn aufdeckbare Pseudonyme vor, unter denen signaturgesetzkonform digital signiert werden kann.[502]

Hinsichtlich der Möglichkeit, durch die Verwendung des Pseudonyms und die dabei entstehenden Datenspuren den Personenbezug aufzudecken, sind *Transaktionspseudonyme*, die nur für eine Transaktion benutzt werden, und *Rollenpseudonyme*, die in einer bestimmten Rolle vielfach benutzt werden, zu unterscheiden.[503] Diese ermöglichen eine Wiedererkennung des Pseudonymträgers. Zertifizierte Pseudonyme ermöglichen dem Handelnden, sich ein bestimmtes Attribut (Arzt, Rechtsanwalt, Abgeordneter des Bundestags) bestätigen zu lassen (*qualifizierte Pseudonyme*) und mit diesem im Rechtsverkehr beispielsweise in ihrer jeweiligen Rolle pseudonym zu handeln.

In der Gestaltung der Datenverarbeitungsprozesse und -systeme ist darauf zu achten, diejenigen Formen anonymen und pseudonymen Handelns auszuwählen, zu nutzen oder zu ermöglichen, die der Vermeidung des Personenbezugs und dem Schutz der informationellen Selbstbestimmung am besten gerecht werden.

Im Sinn der in Kap. 3.4.2 getroffenen Unterscheidung zur Vermeidung des Personenbezugs ist auch für das Mittel der Verarbeitung anonymer und pseudonymer Daten zu differenzieren:

- Die Verarbeitung personenbezogener Daten ist nicht erforderlich, wenn der Zweck auch mit anonymen oder pseudonymen Daten erreicht werden kann. Daher besteht eine Vermutung, dass die Verarbeitung personenbezogener Daten unzulässig ist, wenn eine Verarbeitung anonymer und pseudonymer Daten möglich ist. Die aus dem Erforderlichkeitsprinzip folgende Pflicht der verantwortlichen Stelle, die Daten anonym oder pseudonym zu erheben oder so früh wie möglich zu anonymisieren oder zu pseudonymisieren, sollte ausdrücklich im Gesetz geregelt werden. Ihre Erfüllung sollte Voraussetzung der Datenverarbeitung sein.
- Von dieser Verarbeitungsvoraussetzung zu unterscheiden ist die Optimierungsanforderung, die Verarbeitungsverfahren und -systeme so zu gestalten, dass sie auch mit anonymen oder pseudonymen Daten arbeiten können. Diese Anforderung steht unter dem Vorbehalt des Möglichen und Verhältnismäßigen.

Die Anforderungen an die Gestaltung der Verfahren und Datenverarbeitungssysteme, die im vorigen und diesem Kapitel erörtert worden sind, könnten etwa in folgender Vorschrift zusammengefasst werden:

---

[500] Eine solche Möglichkeit sieht auch der *AK Technik*, DuD 1997, 711, für die von ihm sogenannten Referenz-Pseudonyme vor. S. hierzu auch die amtliche Begründung zum TDDSG, BR-Drs. 966/96. Bei dieser Art von Pseudonymen kann der Personenbezug nur über entsprechende Referenzlisten hergestellt werden, die vorzugsweise räumlich und organisatorisch getrennt von den pseudonymisierten Daten in einer Vertrauensstelle zu speichern sind.

[501] S. *Roßnagel/Scholz*, DuD 2001, 725.

[502] S. hierzu *Roßnagel*, in: *ders.*, RMD, § 7 SigG, Rn. 34 f.

[503] S. zur weiteren Unterscheidung zwischen öffentlichen Pseudonymen, nicht-öffentlichen und anonymen Pseudonymen z.B. *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 247f.; *Federrath/Pfitzmann* 1998, 324f.; s. zu Pseudonymarten außerdem *Köhntopp* 2000b, 1 ff.; *Clarke* 1999.

(1) Die verantwortliche Stelle hat ihre Verfahren und Datenverarbeitungsysteme so zu gestalten oder auszuwählen, dass sie

1. *keine oder so wenig personenbezogene Daten wie möglich verarbeitet,*
2. *soweit dies nicht möglich ist, einen Personenbezug der Daten so weit wie möglich ausschließt, und,*
3. *soweit beides nicht möglich ist, die personenbezogenen Daten so bald wie möglich löscht, anonymisiert oder pseudonymisiert.*

(2) Die verantwortliche Stelle hat die anonyme oder pseudonyme Nutzung und Bezahlung ihrer Angebote und Leistungen zu ermöglichen, soweit dies technisch möglich und verhältnismäßig ist. Sie hat Interessierte über diese Möglichkeit und über geeignete Vorsorgemaßnahmen zu informieren.

(3) Der Personenbezug sollte soweit möglich

1. *durch anonyme Daten*
2. *soweit dies nicht möglich ist, durch Pseudonyme mit Aufdeckungsmöglichkeit nur durch die betroffene Person und,*
3. *soweit beides nicht möglich ist, durch Pseudonyme mit Aufdeckungsmöglichkeit durch einen vertrauenswürdigen Dritten*

vermieden werden.

Im Rahmen des Forschungsprojekts DASIT[504] wurde in einem Feldtest[505] und in einer Simulationsstudie[506] ein prototypisches Verfahren zum pseudonymen Einkaufen und Bezahlen im Internet erprobt. Verwendet wurden dabei von jedem Teilnehmer zwei verschiedene von einer Zertifizierungsstelle aufdeckbare digitale Pseudonyme. Bei der Erprobung konnte auch der Kauf körperlicher Güter unter Pseudonym und deren Auslieferung ohne Pseudonymaufdeckung realisiert werden: Beim Einkauf unter Pseudonym werden die Daten des Käufers gesplittet. Der Händler erhält nur die Kaufdaten und eine Transaktionsnummer, während dem Logistikunternehmen nur Name und Lieferanschrift sowie ebenfalls die Transaktionsnummer mitgeteilt werden. Mit deren Hilfe wird die Lieferung der Ware an den richtigen Empfänger gesteuert. Auch durch das bezahlen der Ware mit Kreditkarte im Rahmen von SET wurde dem Händler die Identität des Kunden nicht offenbart. In der Simulationsstudie konnte außerdem erprobt werden, ob die gefundene Lösung auch bei rechtlichen Komplikationen tauglich ist. Sie konnte im Ergebnis Datenschutz in vielfältigen – provozierten – Situationen bieten wie Anfechtung, Widerruf, Wandlung, Minderung, Nachbesserung und Schadensersatz sowie beim Geltendmachen von Datenschutzrechten wie Einsicht in die gespeicherten Daten, Widerruf der Einwilligung sowie Antrag auf Berichtigung und Löschung.[507]

---

[504] Das Forschungsprojekts „DASIT – Datenschutz in Telediensten am Beispiel von Einkaufen und Bezahlen im Internet“ wird von der Deutschen Genossenschaftsbank Frankfurt als Konsortialführer zusammen mit dem Institut für Sichere Telekooperation der Fraunhofergesellschaft Darmstadt und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel durchgeführt. Es ist Teil des Förderschwerpunkts „VERNET – Sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen“ des Bundesministeriums für Wirtschaft und Technologie.

[505] Im Feldtests führten über 50 ausgewählte Nutzer vom 14.5 bis zum 15.6.2001 rund 2000 Kauftransaktionen durch.

[506] Die Simulationsstudie fand mit 13 Teilnehmern am 18./19.6.2001 im Telekooperationslabor des Instituts für Sichere Telekooperation der Fraunhofergesellschaft Darmstadt statt.

[507] S. zu DASIT z.B. *Grimm/Löhndorf/Scholz*, DuD 1999, 272; *Grimm/Löhndorf/Roßnagel* 2000; www.dasit.myshop.de und www.uni-kassel.de/fb10/oeff_recht/projekte/projekteDasitProjekt.ghk und www.sit.fraunhofer.de/MINT/index.html.

Da – wie es die Definition verlangt – Daten nur anonym sind, wenn es praktisch ausgeschlossen ist, einen Personenbezug herzustellen, sind anonyme Daten keine personenbezogenen Daten. Das Gleiche gilt für pseudonyme Daten – mit Ausnahme für den Kenner der Zuordnungsregel. Sie bieten für die verantwortliche Stelle den Vorteil, dass für diese Daten nicht die allgemeinen Datenschutzregeln gelten.[508]

Aber: Auch wenn anonyme und pseudonyme Daten[509] keine personenbezogenen Daten sind und daher die Regelungen zur „Gefahrenabwehr" des allgemeinen Datenschutzes auf sie keine unmittelbare Anwendung finden, sind Vorsorgeregelungen notwendig, um die Eigenschaft der Daten zu sichern, anonym oder pseudonym zu sein. Wenn für Anonymität und Pseudonymität aus Praktikabilitätsgründen ein – nicht zu führender – Nachweis vollständiger Sicherheit vor Re-Identifizierung nicht verlangt werden kann, sondern der praktische Ausschluss einer Personenbeziehbarkeit ausreichen muss, ist es erforderlich, die möglichen Schwachstellen anonymer und vor allem pseudonymer Datenverarbeitung und die möglichen Folgen einer Re-Identifizierung in die rechtliche Regelung einzubeziehen. Auch wenn für den spezifischen Datenverwender heute die Personenbeziehbarkeit dieser Daten praktisch ausgeschlossen werden kann, können Änderungen in den Randbedingungen der Datenverarbeitung und mit ihnen Möglichkeiten der Aufdeckung anonymer oder pseudonymer Daten für andere Datenverwender oder zu einem späteren Zeitpunkt nicht ausgeschlossen werden.[510] Eine Zuordnung sowohl von *anonymen* als auch von *pseudonymen* Daten ist beispielsweise möglich durch

- das Erlangen von Zusatzwissen. So kann bei unterschiedlicher Verteilung von Kontextwissen dies zufällig oder absichtlich zusammengebracht werden.
- die Veränderung der Verhältnismäßigkeit der Aufdeckungsanstrengungen. Angaben, die nicht so bedeutsam sind, dass sich der personelle, finanzielle und technische Aufwand für ihre Zuordnung lohnt, könnten künftig so bedeutsam werden, dass sich diese Bewertung für denselben oder einen anderen Datenverwender ändert.
- die Entwicklung neuer technischer Möglichkeiten. Der Aufwand für die Zuordnung könnte sich erheblich verringern, wenn die hierfür notwendigen Techniken oder Methoden erheblich verbessert werden.
- die bewusste oder zufällige Aufdeckung durch den Betroffenen selbst. Zu einer ungewollten Aufdeckung kann es zum Beispiel kommen, wenn Informationen über den Betroffenen auf verschiedene Schichten der Datenkommunikation verteilt sind.

Das Risiko der Aufdeckung verstärkt sich bei der Verwendung von *Pseudonymen* vor allem durch

- die Verkettungsmöglichkeit. Dies gilt insbesondere, wenn das Pseudonym in unterschiedlichen Rollen und Lebenszusammenhängen eingesetzt wird.
- Die Aufdeckungsmöglichkeit der Zuordnungsregel: Es kann nicht ausgeschlossen werden, dass die Zuordnungsregel auch bisher Unwissenden bekannt wird. Dies kann auch durch den Pseudonymträger ungewollt oder gewollt – etwa bei Reklamationen – erfolgen.

Kommt es aber zu einer Aufdeckung des Pseudonyms, weist nicht nur *ein* Datum Personenbezug auf, vielmehr sind *alle* zu diesem Pseudonym gespeicherten Angaben[511] mit einem

---

[508] S. hierzu ausführlich *Roßnagel/Scholz*, MMR 2000, 727f.

[509] Diese insoweit, als die verantwortliche Stelle keine Aufdeckungsmöglichkeit hat.

[510] S. näher *Roßnagel/Scholz*, MMR 2000, 728f.

[511] Nach § 4 Abs. 4 TDDSG und § 13 Abs. 4 MDStV dürfen pseudonyme Daten zu Personenprofilen zusammengeführt werden.

Schlag zuordenbar.[512] Dann aber können viele Schutzmaßnahmen, die das Datenschutzrecht für die Verarbeitung personenbezogener Daten fordert, die aber unterbleiben konnten, weil die anonymen oder pseudonymen Daten keine personenbezogenen Daten waren, nicht mehr sinnvoll nachgeholt werden.[513]

Um es noch einmal dogmatisch klarzustellen: Die dargestellten künftigen und ungewissen Risiken machen zum gegenwärtigen Zeitpunkt, zu dem die Daten mit dem verfügbaren Kontextwissen nicht personenbeziehbar sind,[514] aus pseudonymen Daten keine personenbeziehbaren Daten.[515] Wenn durch eine Verkettung der Daten oder durch Kontextwissen der verantwortlichen Stelle zum gegenwärtigen Zeitpunkt schon ein Personenbezug möglich ist, handelt es sich nicht um pseudonyme, sondern um personenbezogene Daten. Wenn man an dem Begriff der personenbezogenen oder personenbeziehbaren Daten festhalten will, ist eine andere Bewertung nicht möglich.[516] Mit dieser Feststellung sollen die gerade aufgezeigten Risiken dynamischer Veränderungen nicht wieder geleugnet werden. Vielmehr soll darauf aufmerksam gemacht werden, dass die Strategie zu ihrer Bekämpfung nicht in einer Verbiegung des Begriffs personenbezogener Daten liegen kann.[517] Vielmehr sind gegenüber künftigen und ungewissen, aber doch beachtlichen Risiken – wie auch sonst in der Rechtsordnung – Vorsorgemaßnahmen erforderlich.[518]

Um also ausreichenden Schutz für die informationelle Selbstbestimmung zu gewährleisten, sind datenschutzrechtliche Regelungen notwendig, die Vorsorge gegen die Aufdeckungsrisiken und ihre Folgen für Daten bieten, die keine personenbezogenen Daten sind, aber zu solchen werden können.[519] Notwendig sind Regelungen zur

- Transparenz

  Vor dem anonymen oder pseudonymen Handeln ist die betroffene Person über den Schutz und die Risiken für ihre informationelle Selbstbestimmung aufzuklären. Vor allem ist wichtig, dass sie erfährt, welche Maßnahmen sie ergreifen kann oder vermeiden muss, um eine Aufhebung der Anonymität zu verhindern. Bei Pseudonymen sind Hinweise zur Sicherheit der Zuordnungsregel und ihrer Gewährleistung erforderlich. So ist zum Beispiel bedeutsam, dass die betroffene Person sowohl über die Risiken der Verkettung und nachträglicher Pseudonymaufdeckung als auch über die Möglichkeiten ihrer Vermeidung durch

---

512 S. näher *Roßnagel/Scholz*, MMR 2000, 729.

513 Zu den Rechtsfolgen einer nachträglichen Aufdeckung eines Pseudonyms s. S. näher *Roßnagel/Scholz*, MMR 2000, 730.

514 S. oben die Definition: bei pseudonymen Daten ist ein Personenbezug praktisch ausgeschlossen.

515 S. hierzu ausführlich *Roßnagel/Scholz*, MMR 2000, 726.

516 Zwar ist es möglich, einen Nutzer mit Hilfe seines Pseudonyms zu adressieren und ihm unerwünschte auf sein Profil zugeschnittene Nachrichten oder manipulative Bannerwerbung zu senden. Dadurch kann ein Eingriff in die Privatsphäre gegeben sein, ohne dass die verantwortliche Stelle den Personenbezug herstellt. Dies ist aus datenschutzrechtlicher Sicht aber nur die andere Seite des mit Pseudonymen erstrebten Vorteils, im Internet ohne Personenbezug in allen Formen agieren zu können, ohne sich identifizieren zu müssen. Wenn – wie im Forschungsprojekt DASIT erprobt, s. hierzu oben – unter Pseudonym auch Verträge angefochten und zurück abgewickelt werden können, dann ist es erwünscht, auch unter Pseudonym adressiert zu werden. Unerwünschten Werbenachrichten sollte nicht durch eine dogmatisch nicht vertretbare Ausweitung des Begriffs der personenbezogener Daten, sondern durch eine Anwendung der Regelungen zur kommerziellen Kommunikation auch auf Pseudonyme begegnet werden.

517 Die folgenden Regelungsvorschläge ergeben sich daher nicht aus einer Anwendung geltenden Datenschutzrechts auf pseudonyme Daten, sondern erfordern eigenständige Vorsorgeregelungen.

518 S. zum insoweit strukturgleichen Verhältnis zwischen grundrechtlicher Schutzpflicht und verwaltungsrechtlicher Vorsorge für das Umweltrecht z.B. *Roßnagel*, in: *Koch/Scheuing*, GK-BImSchG, § 5 Rn. 126, 131, 437 ff., 443 ff., 519.

519 S. hierzu auch Teil 3 Kap. 2.1; s. hierzu z.B. auch *Bizer* 1992, 153 ff.; *BVerfGE* 65, 1 (49); *BVerfG*, NJW 1987, 2805 (2806).

Transaktionspseudonyme unterrichtet wird. Im Multimediarecht ist diese präventive Transparenz bereits in § 4 Abs. 1 Satz 2 TDDSG und § 13 Abs. 1 Satz 2 MDStV vorgesehen. Danach haben die Anbieter von Multimediadiensten den Nutzer über die Möglichkeiten zu informieren, die Dienste anonym oder unter Pseudonym in Anspruch zu nehmen und zu bezahlen. Diese Information darf sich aber nicht auf das bloße „Ob" beschränken, sondern muss hinsichtlich des „Wie" auch die genannten Erläuterungen enthalten. Für die Verwendung von anonymen und pseudonymen Daten sind in einem modernisierten BDSG vergleichbare – oder besser präzisere – Informationspflichten vorzusehen.[520]

Wenn die Anbieter von ihnen generierte Pseudonyme verarbeiten, müssen sie in der Unterrichtung darauf hinweisen oder nachträglich darüber unterrichten, wenn dies dem Pseudonymträger nicht ohnehin bekannt ist. Nachträglich ist bei Pseudonymen erforderlich, dass ihr Träger Informationen über ihre Verwendung durch ein Auskunftsrecht erhalten kann.[521] Ohne die vorhergehende Information über die Verarbeitung von Pseudonymen könnten ihre Träger dieses Recht nicht geltend machen.[522]

- Sicherung der Anonymitäts- und Pseudonymitätseigenschaft

  Um die Eigenschaft der Daten, anonym und pseudonym zu sein, nicht zu gefährden, sind Vorsorgemaßnahmen notwendig, die zum Einen die Wahrscheinlichkeit ihrer Personenbeziehbarkeit vermindern und zum Anderen das Schadenspotenzial einer Aufdeckung reduzieren.

  Pseudonyme Profile[523] sollten entsprechend der Regelung in § 4 Abs. 4 TDDSG und § 13 Abs. 4 MDStV zwar grundsätzlich zulässig sein. Durch die Verkettung vieler Aktivitäten in einem Profil steigt jedoch das Risiko der Aufdeckung des Pseudonyms beträchtlich.[524] Daher ist für das Bundesverfassungsgericht „eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen ... *auch in der Anonymität* statistischer Erhebungen unzulässig."[525] Aber auch soweit das Profil zulässig ist, weil es nicht zu der verfassungswidrigen umfassenden Registrierung und Katalogisierung der Persönlichkeit führt, bleibt ein regelungsbedürftiges Aufdeckungsrisiko, das Vorsorgemaßnahmen zur Sicherung der informationellen Selbstbestimmung erforderlich macht. Wie bei identifizierten Profilen[526] ist daher zu fordern, dass – soweit dies möglich ist – der Träger des Pseudonyms über die Profilbildung unterrichtet wird und die Möglichkeit hat, der Profilbildung zu widersprechen.[527]

  § 4 Abs. 4 Satz 2 TDDSG und § 13 Abs. 4 Satz 2 MDStV sehen für unter Pseudonym erstellte Nutzungsprofile als weitere Vorsorgeregelung bereits vor, dass die nachträgliche Herstellung des Personenbezugs ausdrücklich für unzulässig erklärt wird.[528] Ähnlich for-

---

520 S. hierzu den Formulierungsvorschlag im Text oben.

521 S. Teil 3 Kap. 7.1.1 und 7.1.3.

522 S. zur Unterrichtung bei pseudonymer Profilbildung im Folgenden.

523 S. hierzu auch *Schaar*, DuD 2001, 382 ff.

524 *AK Technik* (o. Fußn. 19), DuD 1997, 711.

525 *BVerfGE* 65, 1 (53), Hervorhebung durch die Verfasser.

526 S. Teil 3 Kap. 3.5.4.

527 S. näher zu dem in § 6 Abs. 3 TDDSG-E geregelten Widerspruchsrecht *Schaar*, DuD 2001, 386f.

528 Will man auf die Vorteile eines geregelten Aufdeckungsverfahrens nicht verzichten muss der Pseudonym-Träger die Möglichkeit haben, nach der Aufdeckung die Weiternutzung des Profils durch seinen Einwand zu verhindern. Dies wird durch die in Teil 3 Kap. 4.5.4 vorgeschlagenen Regelungen gewährleistet. Lediglich die für die weitere Rechtsverfolgung notwendigen Daten dürfen dann nach dem Regelungsvorschlag in Teil 3 Kap. 3.1.4 weiter verarbeitet werden.

dert § 11 Abs. 6 LDSG Schleswig-Holstein, dass pseudonymisierte Daten nur von solchen Stellen verarbeitet werden dürfen, die keinen Zugriff auf die Zuordnungsfunktion haben.

Auch sind Regelungen zur Übermittlung der anonymen oder pseudonymen Daten erforderlich, durch die die Relativität des Personenbezugs berücksichtigt und eine Neuprognose gefordert wird, ob auch bei dem Empfänger die Zuordnung zu einer bestimmten Person praktisch ausgeschlossen ist. Hier könnte zum Beispiel § 11 Abs. 6 Satz 2 LDSG Schleswig-Holstein ein Vorbild sein. Danach ist die Übermittlung pseudonymisierter Daten nur zulässig, wenn die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.[529] Allein auf die Zuordnungsregel abzustellen, ist jedoch nicht ausreichend, wenn etwa bei detaillierten pseudonymen Profilen der Empfänger auf Grund seines Kontextwissens die Identität auch ohne Kenntnis der Zuordnungsregel aufdecken könnte. Daher muss die übermittelnde Stelle prüfen, ob Anhaltspunkte für eine Aufdeckbarkeit des Pseudonyms beim Empfänger bestehen. Wenn dies der Fall ist, darf die Übermittlung nur mit Einwilligung des Pseudonymträgers erfolgen. Notwendig ist auch eine Bewertung, ob die Übermittlung als Pseudonym notwendig ist oder ob nicht eine Übermittlung anonymer Daten ausreicht, die keinen Bezug zu einer Person über eine Zuordnungsregel mehr zulassen.[530]

- Technisch-organisatorische Sicherungen

  Auch sollten – im Rahmen des Datenschutzmanagementsystems[531] – Pflichten zur Beobachtung der Risiken künftiger Aufdeckungswahrscheinlichkeit und zur Vorsorge gegen Aufdeckungsmöglichkeiten vorgesehen werden. Die Wahrscheinlichkeit der Aufdeckung anonymer oder pseudonymer Daten kann vor allem durch organisatorische und technische Sicherungsmaßnahmen gemindert werden, wie zum Beispiel die von den übrigen Angaben getrennte Speicherung der Identifikationsmerkmale beziehungsweise bei Pseudonymen die gesonderte Aufbewahrung der Zuordnungsregel, wie sie § 4 Abs. 4 TDDSG und § 13 Abs. 4 MDStV bereits vorsehen, oder die Gewährleistung der Vertraulichkeit und Integrität der Daten.

- Aufdeckungsverfahren

  In gewisser Weise eine Vorsorgeregelung stellt auch das geordnete Verfahren zur Aufdeckung von Pseudonymen dar, das erforderlich ist, wenn ein Pseudonymträger wegen Verletzung von Rechtspflichten zur Verantwortung gezogen werden muss. Die hierfür notwendigen Regelungen werden in Kap. 5.2 beschrieben.

Die erforderliche Vorsorge könnte etwa wie folgt geregelt werden:

(1) Eine verantwortliche Stelle, die Pseudonyme verarbeitet, hat soweit möglich den Träger des Pseudonyms darüber entsprechend § X zu unterrichten.

(2) Die verantwortliche Stelle darf pseudonyme Persönlichkeitsprofile erstellen, sofern sie den Träger des Pseudonyms zuvor unterrichtet (§ X) und dieser dem nicht widerspricht. Pseudonyme Persönlichkeitsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammen geführt werden.

(3) Pseudonyme Daten dürfen verarbeitet werden, wenn die verantwortliche Stelle keinen Zugriff auf die Zuordnungsfunktion hat. Sie dürfen ohne Einwilligung des Pseudonymträgers

---

529 S. auch die Begründung in LT-Drs. SH 14/1738, 55f.

530 Z.B. ist die Übermittlung von Nutzungsdaten zum Zweck der Marktforschung nach § 6 Abs. 5 TDDSG-E nur anonymisiert, also ohne jeden Personenbezug und ohne Pseudonym, zulässig – s. *Schaar*, DuD 2001, 386.

531 S. Teil 3 Kap. 4.1.

nur dann übermittelt werden, wenn die übermittelnde Stelle sich zuvor davon überzeugt hat, dass dem Empfänger die Zuordnung des Pseudonyms zu seinem Träger praktisch ausgeschlossen ist.

3.5 Zweckbindung

Die informationelle Selbstbestimmung wird dann gewahrt, wenn die Zwecke respektiert werden, zu deren Erfüllung die betroffene Person in die Datenverarbeitung eingewilligt hat. Sie muss sich der gesetzlich erlaubten Datenverarbeitung nur in dem Ausmaß beugen, in dem die Datenerhebung zur Erreichung eines bestimmten erlaubten Zwecks erforderlich war.[532] Für die informationelle Selbstbestimmung sind nicht nur die Daten, sondern vor allem Verarbeitungszweck und -kontext entscheidend.

Die gesetzliche Ausgestaltung der Zweckbindung soll sicherstellen, dass der Einzelne darauf vertrauen kann, dass die Datenverarbeitung nur zu dem von ihm oder dem Gesetz erlaubten Zweck erfolgt. Ihm soll möglichst genau bekannt sein „wer was wann und bei welcher Gelegenheit über ihn weiß“,[533] damit er sein Verhalten unabhängig von der Furcht, registriert zu werden, wählen und einrichten kann.[534] Oder negativ ausgedrückt: Es muss verhindert werden, dass er zum Objekt einer Datenverarbeitung wird, die er aufgrund ihrer Komplexität und Intransparenz weder beeinflussen noch überblicken kann.[535]

Die Zweckbindung ist nicht auf den öffentlichen Bereich begrenzt.[536] Vielmehr fordert der Schutz der Grundrechte die Zweckbindung ebenso für den nicht öffentlichen Bereich. Auch die DSRL hält in Art. 6 Abs. 1 b) an der Zweckbindung fest und schreibt sie gleichermaßen für den öffentlichen und den nicht öffentlichen Bereich vor.

Die Zweckbindung bestimmt Ziel und Umfang zulässiger Datenverarbeitung und begrenzt sie zugleich auf diese. Eine Verarbeitung personenbezogener Daten darf nur zu bestimmten, in der Einwilligung oder der gesetzlichen Erlaubnis ausdrücklich genannten und legitimen Zwecken erfolgen. Die Datenverarbeitung muss sich an den Zweck halten, zu dem die Einwilligung oder das Gesetz die Datenverarbeitung erlaubt. Eine Datenverarbeitung zu anderen Zwecken ist unzulässig und bedarf der Einwilligung der betroffenen Person. Ob die Datenverarbeitung sich im Rahmen der Zweckbestimmung hält, ist für jede Phase und Form der Datenverarbeitung gesondert festzustellen.

Je nach Konkretisierung kann die Zweckbindung unterschiedlich eng oder weit konzipiert werden. Ein nicht allzu enges Verständnis des Zweckbindungsgrundsatzes enthält die Forderung des Art. 6 Abs. 1 b) DSRL, dass die Datenverarbeitung nicht auf den Zweck beschränkt, sondern mit ihm „vereinbar“ sein muss. Würde diese Formulierung übernommen, würden einige derzeit umstrittene Verarbeitungsformen zulässig, die zwar nicht mit dem Zweck identisch, aber mit ihm zu vereinbaren sind. Das Problem könnte dadurch entschärft werden, dass für spezielle Zwecke, die einwilligungspflichtig sein sollen, „insbesondere“ eine Einwilligung gefordert wird. Dies könnte – wie nach den Regelungen im TKG, dem TDDSG, dem MDStV und der TDSV – zum Beispiel für die Zwecke der Marktforschung, der Werbung und des Marketing gelten.

Allerdings dürften die besseren Gründe dafür sprechen, für die Zweckbindung zu fordern, dass die Datenverarbeitung mit dem Zweck übereinstimmen muss. Die Zweckbindung soll die Steuerung der Datenverarbeitung durch die betroffene Person und den Gesetzgeber ermögli-

---

532 *BVerfGE* 65, 1 (46 ff.); *Mallmann*, CR 1988, 97.

533 *BVerfGE* 65, 1 (43).

534 S. *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 4.

535 S. z.B. *Mallmann*, CR 1988, 97.

536 So aber z.B. *Zöllner*, RDV 1985, 13.

chen und vorhersehbar halten. Jede Aufweichung der Zweckbindung gefährdet dieses Ziel. Umgekehrt bestehen im öffentlichen Bereich mit dem Bezug auf den Antrag oder die Aufgabe der verantwortlichen Stelle ohnehin sehr weite Erlaubnistatbestände, die eine Behinderung der öffentlichen Verwaltung nicht befürchten lassen. Im nicht öffentlichen Bereich sind die gesetzlichen Erlaubnisse zur zwangsweisen Datenverarbeitung zwar stärker eingeschränkt. Diesem Bereich entspricht es aber auch, die Datenverarbeitung stärker auf das Vertragsprinzip zu gründen. Die gewollte Stärkung der Einwilligung ginge wieder verloren, wenn die Bindung an den vereinbarten Zweck gelockert und neben den gesetzlichen Erlaubnistatbeständen weitere Datenverarbeitungen zulässig wären. Die ohnehin kaum erreichbare Vorhersehbarkeit der vielfältigen, umfangreichen und komplexen Verarbeitungen von Daten für die betroffene Person wäre gefährdet, wenn die Einwilligung und die gesetzlichen Erlaubnistatbestände von der verantwortlichen Stelle ausgeweitet werden könnten.

Nicht nur mit dem Erforderlichkeitsprinzip,[537] sondern auch mit dem Grundsatz der Zweckbindung ist

> „die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren."[538]

Dieses „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat"[539] darf nur ausnahmsweise – wie etwa für statistische Datensammlungen – und unter zusätzlichen Garantien durchbrochen werden.

Zur Absicherung der Zweckbindung hält das Bundesverfassungsgericht einen „Schutz gegen Zweckentfremdung durch ... Verwertungsverbote (für) erforderlich."[540] Dies ist konsequent: Wenn eine Datenverarbeitung, die sich nicht im Rahmen des erlaubten Zwecks hält, rechtswidrig ist, muss die Rechtsfolge dieser rechtswidrigen Datenverarbeitung sein, dass die so erlangten Daten nicht rechtswirksam verwertet werden dürfen. Das Recht darf keinen Anreiz setzen, gegen seine eigenen Vorgaben zu verstoßen. Dies gilt auch für die Datenverarbeitung mit nicht gezielter Datenverarbeitung.[541] Ausnahmen – etwa im Bereich der Strafverfolgung – können im unvermeidbaren Umfang in bereichsspezifischen Regelungen vorgesehen werden.

Das Niederländische Datenschutzgesetz[542] sieht in Art. 7 ohne Differenzierung nach öffentlichem und nicht öffentlichem Bereich vor, dass die Datenerhebung nur zu bestimmten, ausdrücklich genannten und legitimen Zwecken erfolgen darf. Die weitere Datenverarbeitung muss nach Art. 9 Abs. 1 mit diesem Zweck vereinbar sein. Für die Bestimmung der Vereinbarkeit werden in Art. 9 Abs. 2 als Kriterien genannt: die Beziehung zwischen dem Zweck der beabsichtigten Verarbeitung und dem Zweck zu dem die Daten erhoben wurden, der Charakter der Daten, die Konsequenzen der beabsichtigten Verarbeitung für die betroffene Person, die Art und Weise wie die Daten erhoben und der Umfang angemessener Maßnahmen, die zum Schutz der betroffenen Person ergriffen wurden.

Auch das künftige allgemeine Datenschutzgesetz Japans sieht vor, dass der Personal Information Database Holder den Zweck der Datenverarbeitung genau spezifizieren und sich die Erhebung und Verarbeitung der Daten im Rahmen dieser Zweckbestimmung halten muss. Allerdings ist eine Zweckänderung bereits dann zulässig, wenn sie allgemein akzeptabel ist

---

537 S. Teil 3 Kap. 4.

538 *BVerfGE* 65, 1 (46); s. ferner *Geiger*, in: *Simitis* u.a., BDSG, § 13 Rn. 26 m.w.N.

539 *BVerfGE* 65, 1 (47).

540 *BVerfGE* 65, 1 (46).

541 S. Teil 3 Kap. 2.6

542 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

und sich in einem vernünftigen Rahmen hält. Unzulässige Zweckänderung kann auf Antrag der betroffenen Person zur Löschung oder Sperrung verpflichten.[543]

3.5.1 Datenverarbeitung mit gezieltem Personenbezug

Die normale Datenverarbeitung mit gezieltem Personenbezug[544] wird also durch den in der Einwilligung, im Vertrag, im vertragsähnlichen Vertrauensverhältnis, im Antrag oder in einem anderen gesetzlichen Erlaubnistatbestand genannten Zweck begrenzt.

Wie bereits Art. 6 Abs. 1 b) DSRL und seine Umsetzung in § 28 Abs. 1 Satz 2 BDSG fordern, sollte die verantwortliche Stelle bei der ersten Datenverarbeitung den Zweck eindeutig festlegen.[545] Dies bedeutet, dass sie zumindest bei der Inanspruchnahme eines Erlaubnistatbestands den Zweck hinsichtlich des konkreten Verwendungszwecks präzisieren muss.

Da die Datenverarbeitung aber in allen ihren Phasen dieser Zweckbestimmung entsprechen muss, hat die verantwortliche Stelle diese Prüfung bei jeder weiteren Phase durchzuführen.

Zweckbegrenzung und Zweckbindung werden soweit möglich durch das genutzte Datenverarbeitungssystem und die Organisation des Verarbeitungsprozesses[546] gewährleistet.

3.5.2 Datenverarbeitung ohne gezielten Personenbezug

Die Datenverarbeitung ohne gezielten Personenbezug verfolgt den Zweck, technische Dienstleistungen der Telekommunikation, technische Kommunikation zwischen automatisch tätigen Maschinen oder Verfahren zur Suche nach Informationen zu ermöglichen.[547] Die technische Dienstleistung, leitungsgebundene und mobile Telekommunikation zu ermöglichen, erfordert die Verarbeitung einer gewaltigen Menge von Daten. Diese wird vervielfacht durch das technische Ermöglichen, im Cyberspace zu handeln. Sie wird potenziert, wenn die unübersehbare Vielfalt des Ubiquitous Computing in der Alltagswelt hinzu kommt.[548] Diese Daten sind als personenbeziehbar anzusehen.

Diese Formen der Datenverarbeitung und die von ihnen verarbeiteten Daten haben einen sehr unterschiedlichen Doppelcharakter:

Solange diese Daten allein in dem jeweiligen technischen System erzeugt, verarbeitet und danach sofort wieder gelöscht werden, geht von ihnen kein abzuwehrendes Risiko für die informationelle Selbstbestimmung aus.[549] Dies wurde auch für die aus verarbeitungstechnischen Gründen vorübergehend erstellten Dateien so gesehen, die § 1 Abs. 3 BDSG 1990 sogar völlig aus dem Anwendungsbereich des Gesetzes heraus nahm.[550] Zu gewährleisten ist daher nur, dass die Datenverarbeitung inhaltlich, strukturell und zeitlich auf diese technische Datenver-

---

543 Japanische Expertenkommission 2000, 6, 11.

544 S. Teil 3 Kap. 2.6.

545 Kritisch zur Verwendung des Begriffs „konkret“ statt „eindeutig“ *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 11.

546 S. zum Datenschutzmanagementsystem Teil 3 Kap. 4.1.

547 S. Teil 3 Kap. 2.6.

548 S. Teil 1 Kap. 1.2.

549 *Bull*, RDV 1999, 150 bezeichnet solche rein technisch notwendigen Daten als „belanglos“.

550 S. z.B. *Simitis*, in: *ders. u.a.*, BDSG, § 1 Rn. 229 ff.; *Schaffland/Wiltfang*, § 1 Rn. 23: keine Gefahr für eine Beeinträchtigung des Persönlichkeitsrechts.

arbeitung begrenzt bleibt. Dies wird durch die in Kap. 2.6 genannten Anforderungen sichergestellt. Sie werden unterstützt durch eine Bußgeldregelung und ein Verwertungsverbot.[551]

Sobald aber die Daten das jeweilige technische System verlassen und für andere Zwecke verwendet werden, ermöglichen sie sehr aussagekräftige Aussagen über potenziell jede Lebensregung der betroffenen Person. Es geht dann nicht mehr nur um Kommunikationsbeziehungen oder Kommunikationsinhalte, sondern auch um alle Handlungen, die im Cyberspace vollzogen werden, und schließlich alle Lebensvollzüge, bei denen in irgendeiner Form Objekte beteiligt sind, die Signale aussenden, empfangen oder verarbeiten können. Sie müssen daher als sehr riskant eingestuft werden. Soll die notwendige Unbefangenheit in der Nutzung der Technik gewährleistet werden, soll verhindert werden, dass potenziell jede Lebensäußerung auswertbar ist, muss als Reaktion auf das Eindringen der Informationstechnik in alle Lebensbereiche die eindeutige Entscheidung getroffen werden, dass die Daten ohne Ausnahme nach der Erfüllung des technischen Zwecks sofort gelöscht werden.

Die in Kap. 2.6 vorgestellte Regelung kann daher nur unter den dort genannten Voraussetzungen gelten. Wer diese Anforderungen nicht erfüllt, wer vor allem einen weitergehenden Zweck mit diesen Daten verfolgt, etwa sie für die Abrechnung zu verwenden, muss von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug einhalten. Ergibt sich die Absicht einer weiteren Verwendung der Daten im Einzelfall erst nachträglich, ist dies nur zulässig, wenn diese Zweckänderung nach allgemeinen Anforderungen zulässig ist,[552] also durch eine Einwilligung oder einen Erlaubnistatbestand gedeckt ist und die Voraussetzungen erfüllt, die Daten nicht bei der betroffenen Person erheben zu dürfen.

Könnten sich durch die gesonderte Regelung der Datenverarbeitung ohne gezielten Personenbezug, wie sie in Kap. 2.6 vorgestellt wurde, besondere Probleme durch eine mögliche Zweitverwertung durch Sicherheitsbehörden ergeben? Zwei Problembereiche sind zu betrachten: Das erste Problem ergäbe sich durch eine Verpflichtung der Datenverarbeiter, die Daten zu Zwecken der Strafverfolgung oder im Interesse der öffentlichen Sicherheit länger als notwendig aufzubewahren. Das zweite Problem könnte sich dadurch ergeben, dass für diese Zwecke Echtzeit-Kontrollmöglichkeiten geschaffen werden müssen.

Hinsichtlich des ersten Problems ist – entsprechend den obigen Ausführungen – strikt von dem Grundsatz auszugehen, dass die Fristen für die Speicherung der Daten allein durch den Primärzweck, nicht aber durch Kontrollbedürfnisse bestimmt werden dürfen.[553] Auch für die aus verarbeitungstechnischen Gründen vorübergehend erstellten Dateien wurde von § 1 Abs. 3 BDSG 1990 gefordert, dass sie automatisch sofort nach Abschluss des Verarbeitungsprozesses gelöscht werden müssen. Nach diesem Grundsatz können Sicherheitsbehörden – bei Vorliegen der rechtlichen Voraussetzungen – Daten verarbeiten, die vorhanden sind, nicht aber – allein zu diesem Zweck – die Speicherfrist für die Daten beim Datenverarbeiter bestimmen. Dieser Grundsatz korrespondiert bei der Datenverarbeitung ohne gezielten Personenbezug auch mit den Rechten der betroffenen Person. Wenn diese zur Entlastung des Da-

---

[551] Die Dateien sollten zusammen mit den Protokoll-, Betriebs- und Sicherungsdaten nach §§ 14 Abs. 4 und 31 BDSG rechtlich auf diesen Zweck begrenzt und den Anforderungen an das Datengeheimnis und an die Datensicherung unterworfen werden. Fast alle Datenschutzgesetze schaffen eine besondere Zweckbindung für personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsmäßigen Betriebes von Datenverarbeitungsanlagen gespeichert worden sind: § 12 Abs. 4 LDSG BW; Art. 17 Abs.4 BayDSG; § 11 Abs. 5 BlnDSG; § 12 Abs. 4 BrDSG; § 13 Abs. 3 HDSG; § 10 Abs. 4 NDSG; § 13 Abs.5 LDSG Rh.-Pf.; § 12 Abs. 4 SächsDSG; § 10 Abs. 4 DSG LSA; § 9 Abs.5 LDSG SH; § 20 Abs. 4 ThürDSG. Auch die bereichsspezifische Regelung des § 20 Abs. 2 HSOG enthält ein solche Verwendungsverbot.

[552] S. das folgende Kapitel.

[553] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Mai 2001.

tenverarbeiters und zur Vermeidung kontraproduktiver Effekte keinen Auskunftsanspruch hat, dann sollten auch die Ansprüche der Sicherheitsbehörden nicht weiter gehen. Wenn der Auskunftsanspruch leer läuft, weil alle Daten sofort nach der Funktionserfüllung gelöscht werden, dann sollte dies auch für Sicherheitsbehörden gelten.

Das zweite Problem besteht darin, dass die Sicherheitsbehörden unter bestimmten gesetzlich geregelten Voraussetzungen[554] heute die Befugnis haben, die Telekommunikation in Echtzeit abzuhören oder sich Doppel der Kommunikation zur Verfügung stellen zu lassen und die gewonnenen Daten zu verarbeiten. Die Telekommunikationsbetreiber haben ihnen hierfür Schnittstellen für die unverschlüsselte Kommunikation anzubieten. Diese Befugnisse sind ein Problem für die strikte Zweckbindung der Daten, begründen aber kein spezifisches Problem für die Datenverarbeitung ohne gezielten Personenbezug. Denn die Daten unterfallen der Überwachungsbefugnis auch dann, wenn sie gezielt erhoben werden. Ob diese Befugnisse auf alle technisch erfassten Lebensäußerungen ausgedehnt werden sollen, ist eine Frage der Abwägung zwischen Datenschutz und innerer Sicherheit, die im bereichsspezifischen Datenschutz zu entscheiden sein wird.

3.5.3 Zweckänderung

Da jede Zweckänderung ohne Einwilligung ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung ist, darf sie nur zugelassen werden, wenn dafür eine gesetzliche Ermächtigung vorgesehen worden ist.[555] Zweckändernde Verarbeitungen dürfen daher zulässig sein, soweit gesetzliche Ermächtigungen die Durchbrechung der Zweckbindung ausdrücklich gestatten. Jedes personenbezogene Datum kann – abhängig von seiner Verwendung – für den Betroffenen, seinen sozialen Geltungsanspruch und seine Außenwirkung Relevanz erlangen. Beispielsweise kann selbst ein auf den ersten Blick belangloses Datum wie die Adresse im Rahmen moderner Scoring-Verfahren für die Kreditwürdigkeit entscheidende Bedeutung erhalten.[556] Der Verwendungszweck ist deshalb besonders unter den Bedingungen der allgemeinen Verbreitung der automatisierten Datenverarbeitung und der tendenziell ubiquitären Datennutzung entscheidend für die informationelle Selbstbestimmung geworden.[557]

Da die zweckändernde Datenverarbeitung nicht mehr vom bisherigen Zweck gedeckt ist, sondern eine „neue“ Datenverarbeitung ist, müssen für diese alle Voraussetzungen erfüllt werden wie für die erstmalige Datenverarbeitung. Dies heißt, sie ist zulässig, wenn sie auf eine Einwilligung der betroffenen Person gestützt werden kann oder von einem Erlaubnistatbestand[558] gedeckt ist. Da sie ohne Mitwirkung der betroffenen Person erfolgt, ist sie außerdem nur zulässig, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder der zulässige Verarbeitungszweck[559] eine solche Erhebung erforderlich machen.[560] Die Verarbeitung von Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung sowie zu Organisationsuntersuchungen gilt nicht als Verarbeitung für einen anderen Zweck.

Im öffentlichen Bereich muss demnach die Zweckänderung für die Aufgabenerfüllung der verantwortlichen Stelle erforderlich sein. Doch können weder nur möglicherweise eintretende

---

554 Z.B. § 100a StPO, Gesetz zu Art. 10 GG und TKÜV.

555 S. *v. Zezschwitz*, in: *Roßnagel* HB-Datenschutzrecht, Kap. 3.1, Rn. 58.

556 S. *Koch*, MMR 1998, 458 ff., *Petri*, DuD 2001, 290 ff. sowie *Eul*, in: *Roßnagel* HB-Datenschutzrecht, Kap.7.2.

557 S. hierzu *Globig*, in: *Roßnagel* HB-Datenschutzrecht, Kap. 4.7 Rn. 78.

558 S. Teil 3 Kap. 3.1.

559 S. Teil 3 Kap. 3.3.1

560 S. Teil 3 Kap. 3.2.2.

künftige Zwecke noch Zwecke anderer Stellen die Zweckänderung legitimieren. Die Amtshilfe bietet insoweit grundsätzlich auch keine ausreichende Rechtsgrundlage.[561]

Für die Datenverarbeitung im nicht öffentlichen Bereich wurde von einem Arbeitskreis aus Wirtschaftsvertretern auf folgendes Problem hingewiesen: Im Rahmen von Langfristverträgen, wie etwa Versicherungs- oder Kontoführungsverträgen, kann die Zweckbindung der Datenverarbeitung durch Einwilligungen zu schwierigen Situationen für die verantwortliche Stelle führen: So kann es zum Beispiel aus deren Sicht notwendig werden, die Daten im Rahmen der 450 Mio. Versicherungsverträge an neue, in den alten Einwilligungen nicht vorgesehene Empfänger zu übermitteln. Dies ist nicht möglich, wenn nachträglich von allen betroffenen Personen die Zustimmung eingeholt werden soll. Im Regelfall antworten nämlich maximal 30 Prozent der Angefragten positiv auf die Bitte, eine erweiterte schriftliche Einwilligung zu übermitteln. Die Einholung der Einwilligung und das Ergebnis, dass nur eine Minderheit zustimmt, kann große praktische Schwierigkeiten verursachen.

Um diese Probleme zu verringern, könnte an eine Regelung gedacht werden, Schweigen als Einwilligung anzusehen. Aber in diesem Fall müsste eine Widerspruchslösung vorgesehen werden. Diese führt zwar erfahrungsgemäß zu einem Opt-out von höchstens 10 Prozent, doch löst sie das Problem nur graduell und nicht grundsätzlich, da auch sie zu einer nach Zustimmenden und Nicht-Zustimmenden gespaltenen Datenverarbeitung führt.

Eine andere Lösung könnte darin bestehen, dass die Kontrollstelle an Stelle der betroffenen Personen der Zweckänderung zustimmen könnte. Dies wäre allerdings ein massiver Eingriff in die informationelle Selbstbestimmung der betroffenen Personen. Sowohl für diese Lösung wie auch für die Lösung, die Schweigen als Einwilligung wertet, ist nicht recht ersichtlich, wie sie mit dem Prinzip der Privatautonomie vereinbar sein könnte. Für die genannten langfristigen Verträge gilt – wie für alle anderen Vertragsklauseln – das Prinzip der Vertragsbindung und der Vertragsfreiheit. Sie können nur geändert werden, wenn der Kunde ihnen zustimmt. Sie können – ohne entsprechende Vereinbarung – nicht eigenmächtig oder mit Widerspruchslösung geändert werden. Es ist nicht ersichtlich, wieso für die Datenschutzklauseln anderes gelten sollte. Auch für alle anderen Vertragsklauseln ergibt sich das genannte Datenverarbeitungsproblem, ohne dass hierfür die genannten Lösungen zur Anwendung kommen würden.

Als zusätzliche Sicherung gegen voreilige Zweckänderungen sollte – wie etwa in § 13 Abs. 7 LDSG Schleswig-Holstein – gefordert werden, dass jede Zweckänderung dokumentiert werden muss. Dies sicherzustellen, ist eine Aufgabe des Datenschutzmanagementsystems.[562]

Für bestimmte Daten sollte eine Zweckänderung ausgeschlossen werden. Dies kann etwa für besonders schützenswerte Daten, die für bestimmte Zwecke verarbeitet werden, in bereichsspezifischen Regelungen vorgesehen werden. Im allgemeinen Datenschutzgesetz sollte eine solche nicht zu durchbrechende Zweckbindung zumindest für die Daten vorgesehen werden, die ausschließlich

- zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebs eines Datenverarbeitungssystems,
- für Zwecke der Forschung, der journalistisch-redaktionellen Medienarbeit sowie von Warndiensten, Detekteien und Auskunftteien,
- ohne gezielten Personenbezug und

[561] Grundlegend in diesem Zusammenhang *Schlink*, NVwZ 1986, 249 ff.; s. auch die Formulierung in *BVerfGE* 65, 1 (46), wonach ein amtshilfefester Schutz vor Zweckentfremdung erforderlich ist.

[562] S. Teil 3 Kap. 4.1.

- zur Abrechnung von Telekommunikations- und Telediensten

verarbeitet werden.

3.5.4 Profilbildung

Da jedes personenbezogene Datum ein virtuelles Abbild der sozialen Beziehungen darstellt, in denen sich der Einzelne bewegt, lassen sich verfassungsrechtlich zu verhindernde Gesamtbilder nur vermeiden, wenn die über die einzelnen sozialen Beziehungen gespeicherten Daten grundsätzlich von einander getrennt gehalten werden.[563]

Eine besondere Herausforderung dieser Ausprägung der Zweckbindung wird zunehmend der Schutz vor der Bildung und Nutzung von Persönlichkeitsprofilen sein.[564] Dabei dürfte das eigentliche Problem in der Erstellung von Profilstrukturen und der Einbindung einzelner Daten in diese Struktur liegen. In diesem Zusammenhang stellt nicht so sehr das einzelne Datum das Risiko für die informationelle Selbstbestimmung dar, sondern die Gesamtinformation, die sich für die verantwortliche Stelle aus diesem Datum in Kombination mit anderen Daten innerhalb der Datenstruktur und bezogen auf sein Auswertungsinteresse ergibt. Im Internethandel zum Beispiel werden aus einer Vielzahl von für sich genommen möglicherweise harmlosen Einzelinformationen individuelle Nutzer- und Kundenprofile entwickelt, die mit hoher Aussagekraft Präferenzen, Bedürfnisse, Kaufgewohnheiten und sonstige Verhaltensweisen beschreiben.[565]

Durch die Profilbildung ergibt sich zum Einen das Risiko, dass durch das Gewinnen neuer Daten aus der Zusammenführung alter Daten Probleme des Kontextverlusts und der Richtigkeit der neuen Daten entstehen können: Aus dem Vorliegen bestimmter Eigenschaften werden Schlüsse auf das Vorhandensein anderer Eigenschaften gezogen, die mehr oder weniger empirisch belegt sind. Diese neuen Daten werden in Dateien fixiert und bei anderer Gelegenheit als belastbare Daten verwendet – auch für diskriminierende Einstufungen.[566] Es besteht daher die Gefahr, dass die personenbezogenen Daten zu einem Persönlichkeitsprofil zusammengefügt werden, „ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann“.[567]

Zum Anderen entsteht das Risiko, dass aus – unter Umständen sehr umfangreichen und viele Merkmale erfassenden – Datenbeständen für einzelne Lebensbereiche jederzeit beliebige Profile mit einer Vielzahl von Kategorisierungen zu unterschiedlichen Fragestellungen erstellt werden können.[568] Diese vielfältige Reproduzierbarkeit des Persönlichkeitsprofils bewirkt ein Gefühl des Ausgeliefertseins[569] und ein Wissen um die Fremdbeobachtung, die beide zu Ver-

---

563 S. *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 1.

564 S. zur Gefahr der Profilbildung allein bei der Nutzung von Multimedia-Diensten z.B. *Roßnagel/Bizer* 1995, 42f.; *Schaar*, CR 1996, 172; *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, 2887; *Enquete-Kommission* 1998, BT-Drs. 13/11002, 93; *Fiege*, CR 1998, 42; *Engel-Flechsig*, in: *Roßnagel*, RMD, Einl TDDSG, Rn. 70; *Bizer*, in: *Roßnagel*, RMD, § 3 TDDSG, Rn. 136; *Schaar/Schulz*, in: *Roßnagel*, RMD, § 4 TDDSG, Rn. 105ff.; *Gridl* 1999, 75; *Püttmann*, K&R 2000, 494; *Schmitz* 2000, 56; *Ladeur*, MMR 2000, 715 am Beispiel „virtueller Videotheken“. S. auch schon *Roßnagel/Wedde/Hammer/Pordesch* 1990, 221f. mit Bezug auf den traditionellen Geschäftsvorfall außerhalb des Internet. Für die Chipkartentechnologie s. *Weichert*, DuD 1997, 274f. Speziell zu den Gefahren des Online-Profiling s. *U.S. Federal Trade Commission* 2000b; *Kong*, Mercury News 2000, http://www.mercurycenter.com/business/top/060236.htm. S. auch den Gemeinsamen Standpunkt der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation vom Mai 2000 zu „Online Profiles on the Internet“, http://www.datenschutz-berlin.de/IWGDPT/pr_en.htm.

565 S. *Schaar*, DuD 2000, 275 sowie Teil 1 Kap. 2.1.

566 S. näher *Breinlinger*, RDV 1997, 252.

567 *BVerfGE* 65, 1 (53f.).

568 *Podlech/Pfeiffer*, RDV 1998, 146.

569 S. *Schmidt*, JZ 1974, 245.

haltensbeeinflussungen führen können. Dadurch wird der grundrechtlich verbürgte Anspruch, als selbstverantwortliche oder selbstbestimmte Persönlichkeit respektiert zu werden, in Frage gestellt. Für eine eigene Rolleninterpretation in sozialen Zusammenhängen bleibt kein Raum, wenn der Interaktionspartner schon umfassend informiert ist. Genau dies wird mit der Bildung von Persönlichkeitsprofilen provoziert. Die Bildung von qualifizierten Profilen einer Person, insbesondere wenn sie unternehmensübergreifend erhoben werden und damit unterschiedliche Lebensbereiche umfassen, lässt sehr weitgehende Aussagen über die innere Struktur und Befindlichkeiten der Person zu und ist daher im Hinblick auf den Persönlichkeitsschutz äußerst kritisch zu bewerten.

Das Bundesverfassungsgericht hat sowohl das Registrieren und Katalogisieren der ganzen Persönlichkeit[570] als auch das Anfertigen von Teilabbildern der Persönlichkeit gegen den Willen der betroffenen Person als verfassungswidrig bezeichnet.[571] Diese auf den Staat bezogenen Aussagen sind von ihrem Schutzgehalt her grundsätzlich auch auf die Datenverarbeitung nicht öffentlicher Stellen zu übertragen.[572] Zwar führt die starke Ausrichtung des Bundesverfassungsgerichts auf die Gefahr umfassender Persönlichkeitsprofile wenig weiter, weil in der Praxis niemand an der Erstellung von vollständigen Persönlichkeitsbildern interessiert ist.[573] Die Erstellung von Totalbildern, die sämtliche Aspekte der Persönlichkeit erfassen, ist schlicht nicht möglich. Andererseits besteht aber auch kein Zweifel daran, dass mit der umfassenden Aufzeichnung und Auswertung von Interessen und Gewohnheiten etwa bei der Internet-Nutzung zumindest ein Teilabbild der Persönlichkeit angestrebt wird.[574] Wenn auch die meisten Persönlichkeitsprofile[575] mangels Eingriffsintensität nicht als verfassungswidrig zu bezeichnen sind,[576] so benötigen sie doch eine Regelung, um ihren spezifischen Risiken für die informationelle Selbstbestimmung adäquat begegnen zu können.

Um für Persönlichkeitsprofile sinnvolle Regelungen finden zu können, sollten sie wie folgt definiert werden: Ein Profil entsteht dann, wenn über das Zusammenführen von Einzeldaten hinaus zusätzliche, bisher nicht vorhandene Erkenntnisse über die Persönlichkeit der betroffenen Person gewonnen und zu einem (Teil-)Abbild der Persönlichkeit zusammengeführt werden.[577] In der Erzeugung der zusätzlichen, auch der betroffenen Person so vielleicht gar nicht bekannten Daten liegt der entscheidende Unterschied zu einer „bloßen“ Zusammenführung verschiedener Daten in einer Datei. Die Menge der gesammelten Daten ist unter Umständen zwar ausschlaggebend für die Aussagekraft eines Profils. Denn je mehr Daten zur Auswertung herangezogen werden, desto präziser und aussagekräftiger sind die daraus gewonnenen

---

570 *BVerfGE* 27, 1 (6); s. auch *Podlech*, in: AK-GG, Art. 2 I, Rn. 79, 83.

571 *BVerfGE* 65, 1 (53f.).

572 *Gola/Schomerus*, BDSG, § 29 Anm. 4.7: „Die vom BVerfG ... getroffene Aussage muß um so mehr gelten, wenn private Wirtschaftsunternehmen derartige Verarbeitungen zur Befriedigung kommerzieller Interessen betreiben wollen“.

573 Insoweit zutreffend *Ladeur*, DuD 2000, 18. *Podlech/Pfeifer*, RDV 1988, 146 sprechen demgegenüber vom individuellen Gesamtprofil.

574 S. auch *Schmitz* 2000, 137; *Schulz*, Verw 1999, 140f.; dagegen werden die Risiken vernachlässigt von *Bull* 1998, 27 und *Ladeur*, DuD 2000, 18; *ders*., MMR 2000, 715 ff.

575 *Breinlinger*, RDV 1997, 249, die zu Recht darauf hinweist, dass eine menschenunwürdige Klassifizierung kaum darin festzustellen ist, dass zum Beispiel aus Zusammenhängen zwischen Freizeitaktivitäten und Einkommensniveau auf eine größere Wahrscheinlichkeit des Konsums höherwertiger Güter geschlossen wird.

576 Jedenfalls werden die zu erwartenden technischen Fortschritte die Möglichkeit umfassender Persönlichkeitsprofile zunehmend vergrößern– s. hierzu *Podlech/Pfeiffer*, RDV 1998, 146.

577 S. *Wittig*, RDV 2000, 59. Zum Begriff des Persönlichkeitsprofils s. bereits *Bull* 1984, 98f., der zusätzlich die Verwendung technischer Mittel bei der Zusammenführung der Daten voraussetzt; *Podlech*, DVR 1972/73, 157 definiert Persönlichkeitsprofil als „Datensatz über eine Person, der umfassend Auskunft über seine Persönlichkeit gibt.“ S. zu verschiedenen Profilarten auch *Weichert*, in: *Kilian/Heussen*, CompHdb, Kap. 130, Rn. 32.

Daten. Für eine Begriffsbestimmung ist der quantitative Maßstab jedoch untauglich. Nur wenn die gesammelten Daten auf ein bestimmtes Ziel hin – zum Beispiel zur Abbildung der Konsumentenpersönlichkeit – inhaltlich verknüpft und umgestaltet werden, sollte daher von einer Profilbildung gesprochen werden.[578]

Ein Verbot von Persönlichkeitsprofilen – wie es § 12 Abs. 16 Sächs.DSG und § 9 Abs. 2 Satz 2 des Entwurfs eines BDSG von Bündnis90/Die Grünen vorsehen[579] – geht zu weit, weil das Erstellen und Nutzen von Persönlichkeitsprofilen auch im Interesse der betroffenen Person liegen kann (Beispiele: effizientere Gestaltung langwieriger Registrierungsprozeduren, persönlich zugeschnittene Dienstleistungen, persönliche Assistenzsysteme, medizinische Profile).[580] In der Internet-Ökonomie wird außerdem die individuell zugeschnittene – auf Profilen zu thematischen Segmenten beruhende – Dienstleistung oder Produktgestaltung den Regelfall bilden.

Das aus der Zweckbindung und dem Erforderlichkeitsprinzip folgende Verbot einer Datenspeicherung auf Vorrat wirkt sich nicht auf die Profilbildung insgesamt, sondern auf bestimmte Ausprägungen des Profilerstellungsprozesses aus. Denn es können beispielsweise an sich unverdächtige Vertragsdaten für Vertragszwecke gespeichert werden und jederzeit – auch über unterschiedliche Anbieter hinweg – zu einem beliebigen Zweck ausgewertet werden. Möglich ist auch, vorhandene Zusatzinformationen in Dateien, wie zum Beispiel in Word-Dateien, die nur – den betroffenen Personen oft unbekannte – Hilfsinformationen darstellen, nachträglich zu einem Profil zusammen zu führen. Die Werkzeuge für spontane Profilbildungen werden immer besser und ermöglichen ad hoc Auswertungen zu unterschiedlichsten Zwecken. Eine Profilbildung auf Vorrat ist hierfür nicht notwendig. Doch auch das Verbot der Vorratsspeicherung lässt sich umgehen, wenn unverdächtige Daten nach und nach – etwa zum Zweck der Vertragserfüllung – ins Ausland übermittelt und dann dort ausgewertet werden.

Eine Regelung der Profilbildung sollte daher kein Totalverbot enthalten und sich auch nicht auf das Verbot der Vorratsspeicherung verlassen. Sie sollte vielmehr durch eine Kombination von Anforderungen erfolgen, die vor allem Transparenz und Einflussnahme für die betroffene Person gewährleisten:

Die beabsichtigte Profilbildung ist als spezifische Form der Datenverarbeitung in der Datenschutzerklärung mit einem Hinweis auf ihre Struktur und ihren Zweck darzustellen.[581]

Für die weiteren Voraussetzungen einer zulässigen Bildung von Persönlichkeitsprofilen ist zu unterscheiden, ob in die Profilbildung eingewilligt wurde oder nicht:

Soll die Profilbildung durch eine Einwilligung legitimiert werden,[582] müssen folgende Voraussetzungen erfüllt sein:

- Vorherige Unterrichtung der betroffenen Person, die sich auf Struktur und Zweck der Profilbildung erstreckt,

---

578 S. *Wittig*, RDV 2000, 61.

579 *Podlech/Pfeiffer*, RDV 1998, 149, halten Profile schon nach geltendem Recht für verboten.

580 S. dazu *U.S. Federal Trade Commission* 2000b, 8ff.

581 S. Teil 3 Kap. 2.3.

582 Nach *Wittig*, RDV 2000, 62, kann eine auch ansonsten wirksame Einwilligung die Erstellung von Persönlichkeitsprofilen nicht rechtfertigen, weil die betroffene Person nach einer Einwilligung keine Möglichkeit mehr hat, darauf Einfluss zu nehmen, welches Persönlichkeitsbild in den Dateien privater Unternehmen entsteht, dies vielmehr allein zu deren Disposition stehe. Dies verkennt jedoch die Zweckbegrenzung durch Einwilligung und die im folgenden vorgeschlagenen Möglichkeiten der Transparenz und Einflussnahme.

- Ausdrückliche Einwilligung, die die Profilbildung und die mit ihr geplanten Auswertung deckt,
- Die betroffene Person hat jederzeit die Möglichkeit, die Einwilligung für die Zukunft zu widerrufen.

Soll die Profilbildung durch einen Erlaubnistatbestand legitimiert werden, müssen folgende Voraussetzungen erfüllt sein:

- Vorliegen der allgemeinen Zulässigkeitsvoraussetzungen: Der Erlaubnistatbestand muss erfüllt, die Profilbildung von dem zulässigen Zweck gedeckt und für die Zweckerreichung erforderlich sein.
- Unterrichtung der betroffenen Person über die Erstellung des Profils und ihr Widerspruchsrecht sowie Hinweis auf die Datenschutzerklärung,
- Die betroffene Person hat jederzeit das Recht, der Profilbildung zu widersprechen.
- Ausnahmeregelung, sofern durch die Erfüllung dieser Anforderungen der Zweck der zulässigen Datenverarbeitung nicht erreicht werden kann (Beispiel: Zielfahndung des BKA, Detektivarbeit). Die Ausnahmeregelung schränkt nicht die Kontrollbefugnis der Kontrollstellen ein.

Profile können auch zu Pseudonymen erstellt werden.[583] Oft ist diese Form der Profilbildung der gebotene Kompromiss zwischen dem berechtigten Interesse einer verantwortlichen Stelle, ihre Kundschaft oder ihre Klientel kennenzulernen, und dem Schutz der informationellen Selbstbestimmung. Daher erlauben § 4 Abs. 4 TDDSG und § 13 Abs. 4 MDStV die Bildung von Profilen zu Pseudonymen. Auch wenn pseudonyme Daten für diejenigen, die die Zuordnungsregel nicht kennen, keine personenbezogenen Daten sind, ist zu fordern, dass der Träger des Pseudonyms über die Profilbildung zu unterrichten ist. Außerdem ist das in § 6 Abs. 3 des Entwurfs eines novellierten TDDSG enthaltene Recht, der Profilbildung zu widersprechen, ebenso als gebotene Vorsorgemaßnahme zu verallgemeinern.[584]

Das schweizerische Bundesgesetz über den Datenschutz[585] enthält eingehende Regelungen zur Erstellung und Verwendung von Profilen. Art. 3 d) versteht unter „Persönlichkeitsprofil" eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben. Nach Art. 18 Abs. 2 muss die Erhebung eines Persönlichkeitsprofils der betroffenen Person erkennbar sein. Verarbeitet werden dürfen Persönlichkeitsprofile nach Art. 17 Abs. 2 nur, wenn ein Gesetz dies ausdrücklich vorsieht oder dies für eine gesetzlich „klar umschriebene Aufgabe" unentbehrlich ist, der Bundesrat es bewilligt hat oder die betroffene Person eingewilligt hat. Eine Übermittlung ist nach Art. 12 nicht ohne besondere Rechtfertigung zulässig, als die Art. 13 eine Einwilligung, ein Gesetz oder ein überwiegendes privates oder öffentliches Interesse nennt. Durch ein Abrufverfahren darf ein Persönlichkeitsprofil nach Art. 19 Abs. 3 nur zugänglich gemacht werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht.

583 S. hierzu auch *Schaar*, DuD 2001, 382 ff.

584 S. Teil 3 Kap. 3.4.3.

585 Gesetz vom 19.6.1992 (Stand. 7.7.1998).

3.5.5 Zweckbindung und Übermittlung von Daten

Die Übermittlung personenbezogener Daten an Dritte, die nicht durch die Zustimmung oder – im privaten Bereich – den Zweck eines Vertrags[586] oder vertragsähnlichen Vertrauensverhältnisses oder – im öffentlichen Bereich – durch eine Erlaubnisnorm gedeckt ist, stellt eine unzulässige Zweckänderung dar, die nur durch Unterrichtung und Einwilligung der betroffenen Person legitimiert werden kann. Die Weitergabe personenbezogener Daten an einen Dritten stellt unabhängig davon, ob die Daten von dem Dritten zu dem primären Erhebungszweck verwendet werden, immer einen gravierenden Eingriff in die Rechte der betroffenen Person dar, wenn sie ohne ihre Mitwirkung erfolgt und sie deswegen über keine Kontrollmöglichkeiten verfügt. Durch Übermittlungen entsteht das Problem der nicht mehr kontrollierbaren Parallelspeicherungen, für die bestimmte Schutzmaßnahmen wie Verwertungsverbote, Zugriffsbeschränkungen, Auskunftssperren und ähnliche nicht mehr wirken.[587] Auch entsteht die große Gefahr, dass die Betroffenenrechte auf Berichtigung, Sperrung und Löschung ihre Wirksamkeit verlieren, wenn die Kette der Übermittlungen nicht mehr lückenlos nachvollzogen werden kann.

Die Übermittlung sollte daher ohne Unterrichtung verboten sein – es sei denn, die betroffene Person weiß von der Übermittlung durch die Einwilligung, den Vertrag, das vertragsähnliche Vertrauensverhältnis oder die Erlaubnisnorm. Die an vielen Stellen des BDSG[588] vorgesehene Gleichstellung der Nutzung personenbezogener Daten durch die für die Verarbeitung verantwortliche Stelle mit einer Übermittlung dieser Daten an Dritte sollte daher aufgegeben werden. Die Übermittlung muss vielmehr durch die Einwilligung, den Antrag, den Zweck eines Vertrags oder vertragsähnlichen Vertrauensverhältnisses oder durch eine Erlaubnisnorm gedeckt sein.

Sollten spezifische Erlaubnistatbestände für die Übermittlung im allgemeinen Datenschutzrecht geschaffen werden?

Im *öffentlichen Bereich* ist die Übermittlung nach dem hier vorgeschlagenen Konzept ohnehin zulässig, wenn sie im Aufgabenbereich der übermittelnden Stelle liegt und für die Erfüllung der Aufgabe erforderlich ist.

Die Übermittlung personenbezogener Daten von öffentlichen Stellen an öffentliche Stellen ist für den Fall regelungsbedürftig, dass die Übermittlung zwar nicht für die Aufgabenerfüllung der übermittelnden Stelle aber für die Erfüllung einer gesetzlich übertragenen Aufgaben der empfangenden Stelle erforderlich ist, diese die Daten anfordert und ein Ausnahmegrund für die Datenerhebung bei Dritten vorliegt.[589]

Die Übermittlung personenbezogener Daten von öffentlichen Stellen an nicht öffentliche Stellen, die nicht für die Aufgabenerfüllung der übermittelnden Stelle erforderlich ist, muss ebenfalls geregelt werden. Sie ist mit dem Anspruch von Bürgern und Unternehmen auf Zugang zu den bei öffentlichen Stellen vorhandenen Daten abzustimmen. In beiden Fällen geht es um die Frage des Informationszugangs und die Abwägung der Interessen an Öffentlichkeit der Verwaltungsinformationen und dem Schutz der informationellen Selbstbestimmung der be-

---

586 Damit ist der Fall gedeckt: Bucht ein Kunde im Reisebüro eine Urlaubsreise, so überlässt er seine Daten zur Übermittlung an den Reiseveranstalter, der sie an das entsprechende Hotel, die Fluggesellschaft, das Busunternehmen etc. weitergeben muss, weil nur so das Reisebüro seinen Vertragszweck erfüllen kann. Ebenso abgedeckt ist der Fall der Auslandsüberweisung, für deren Umsetzung personenbezogene Daten an eine Mehrzahl von Institutionen des Zahlungsverkehrs übermittelt werden müssen.

587 S. zum Folgenden *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 53.

588 S. § 28 Abs. 1; Abs. 3 Satz 1 sowie Abs. 5 Satz 1 und 2 BDSG.

589 Ähnlich Art 27 Abs. 2 des italienischen Datenschutzgesetzes Gesetz Nr. 675 vom 31.12.1996, der zusätzlich eine Information der Kontrollstelle vor der Übermittlung fordert.

troffenen Personen. Diese Fragen können im Informationsfreiheitsgesetz und im Datenschutzgesetz nicht unterschiedlich geregelt werden. Daher sollte die Übermittlung personenbezogener Daten dann zulässig sein, wenn ein Informationszugang zu diesen Daten nach dem Informationsfreiheitsgesetz zulässig wäre.[590]

Wie in den geltenden Regelungen sollte die Verantwortung für das Vorliegen der Übermittlungsvoraussetzungen grundsätzlich bei der übermittelnden Stelle liegen. Lediglich in dem Fall, in dem eine andere öffentliche Stelle die Daten anfordert, soll diese die Verantwortung tragen. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Datenempfängers liegt, es sei denn, dass ein besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. Damit hat die übermittelnde Stelle auch in diesem Fall ein Prüfungsrecht, das nur in den Fällen zur Pflicht wird, in denen sich Zweifel an der Zulässigkeit der Datenübermittlung für die übermittelnde Stelle aufdrängen.

Abweichungen von diesen Grundsätzen wegen besonderer Risiken der Übermittlungen oder spezifischer Verwaltungsaufgaben – wie etwa bei den vielen öffentlichen Registern – sind in bereichsspezifischen Regelungen aufzunehmen.

Im *nicht öffentlichen Bereich* erscheint eine besondere Regelung nicht erforderlich zu sein. Die Übermittlung ist nach dem hier vorgeschlagenen Konzept zulässig, wenn sie von einer Einwilligung oder einem Erlaubnistatbestand[591] gedeckt ist und die Voraussetzungen für eine Ausnahme von der grundsätzlichen Pflicht, die Daten bei der betroffenen Person zu erheben,[592] vorliegen. Die Privilegierung für Übermittlungen von in Listen oder sonst zusammengefassten gruppenbezogenen Daten wie Name, Titel, Adresse, Beruf, Geschäft und Geburtsjahr zum Zweck der Werbung, der Markt- oder Meinungsforschung nach §§ 28 Abs. 3 Nr. 1 c) und 29 Abs. 2 Nr. 1 b) BDSG ist in den zulässigen Erlaubnistatbeständen des Art. 7 DSRL nicht enthalten und daher europarechtswidrig.[593] Im Regelfall wird sich somit die Erlaubnis zur Übermittlung nach privatrechtlichen Vereinbarungen richten.

In beiden Bereichen darf der Dritte, an den die Daten übermittelt werden, diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung für andere Zwecke wäre nur zulässig, wenn die Voraussetzungen für eine Zweckänderung[594] erfüllt sind.

Der Schutz besonderer Geheimnisse bleibt von diesen Regelungen unberührt.

Die betroffene Person ist entsprechend den in Teil 3 Kap. 3.2.2 vorgeschlagenen Regeln grundsätzlich von der Übermittlung zu unterrichten.

Wie jede Zweckänderung[595] sind auch die Übermittlungen zu dokumentieren. Dies sicherzustellen, ist eine Aufgabe des Datenschutzmanagements.[596] Übermittlungen sind von der übermittelnden Stelle auch deshalb zu protokollieren und für eine bestimmte Frist aufzubewahren, um die Anforderungen erfüllen zu können, der betroffenen Person Auskunft über die Emp-

590 S. hierzu insb. § 5 des IFG.

591 S. Teil 3 Kap. 3.1.4.

592 S. Teil 3 Kap. 3.2.2.

593 Ebenso *Geis*, CR 1995, 175, der aber Art. 7 DSRL für verfassungswidrig hält, weil er diese von der Informationsfreiheit des Art. 5 Abs. 1 gebotene Privilegierung der Datenverarbeitung nicht enthalte. Geis übersieht jedoch, dass diese Privilegierung gegenüber Privaten wegen der eingeschränkten Reichweite des der Informationsfreiheit – s. Teil 3 Kap. 4.2 – verfassungsrechtlich nicht geboten, sondern allenfalls möglich ist.

594 S. Teil 3 Kap. 3.5.3.

595 S.. Teil 3 Kap. 3.5.3.

596 S. Teil 3 Kap. 4.1.

fänger von sie betreffenden Daten zu erteilen und Berichtigungen, Sperrungen und Löschungen den Empfängern nachzumelden.

In den vorbereitenden Gesprächen zu dem Gutachten wurde eine spezifische „Sackgassenregelung“ vorgeschlagen, die die weitere Übermittlung übermittelter Daten verhindern soll. Sie kommt nur für die zwangsweise erhobenen Daten in Frage. Für die Übermittlung, die von einer Einwilligung gedeckt ist, gilt deren Erlaubnis. Für die Datenverarbeitung, die zur Vertragserfüllung oder Antragsbearbeitung notwendig ist, gilt, dass eine Weitergabe im erforderlichen Umfang möglich ist. Bleibt nur noch die unfreiwillige Datenverarbeitung: Auch für die Übermittlung gilt der Grundsatz der Erhebung bei der betroffenen Person. Nur wenn dies bei ihr unmöglich oder zweckvereitelnd wäre, dürfen Daten bei einem Dritten erhoben werden. Für die verbleibenden Fälle müssen die Voraussetzungen der Erlaubnistatbestände privatrechtlicher „Gefahrenabwehr“[597] oder konkreter Aufgabenerfüllung erfüllt sein. Die Weiterverarbeitung ist auf diesen Zweck begrenzt. Die betroffene Person ist zu unterrichten. Zusätzlich sollte die Übermittlung einschließlich ihres Zwecks bei der übermittelnden und empfangenden Stelle protokolliert werden. In diesem Regelungsumfeld erscheint eine spezifische „Sackgassenregelung“ nicht erforderlich.

Das italienische Datenschutzgesetz[598] ermöglicht in Art. 20 die Übermittlung oder Verbreitung personenbezogener Daten durch verantwortliche Stellen des Privatrechts und öffentlich-rechtliche Wettbewerbsunternehmen aufgrund der expliziten Einwilligung der betroffenen Person sowie aufgrund weitgehend der gleichen Erlaubnistatbestände,[599] die nach Art. 12 auch eine Datenverarbeitung ohne Einwilligung der betroffenen Person ermöglichen.[600] Allerdings sind die Erlaubnistatbestände des Vertrags und des vertragsähnlichen Vertrauensverhältnisses und der wissenschaftlichen Forschung nicht aufgeführt.[601] Das italienische Recht vermeidet dadurch eine Generalklausel und ein Abwägungserfordernis zwischen den beteiligten Interessen. Die Übermittlung personenbezogener Daten von öffentlichen Stelle an öffentliche Stellen ist nach Art. 27 Abs. 2 des italienischen Datenschutzgesetzes[602] zulässig, wenn dies gesetzlich vorgesehen ist oder in irgend einer Weise erforderlich ist, um die gesetzlich übertragenen Aufgaben dieser Stellen zu erfüllen. Im zweiten Fall muss die Kontrollstelle vor der Übermittlung informiert werden und kann durch eine begründete Entscheidung eine Übermittlung verhindern, die gegen das Datenschutzgesetz verstößt. Die Übermittlung personenbezogener Daten von öffentlichen Stellen an private Stellen oder öffentlich-rechtliche Wettbewerbsunternehmen ist nach Art. 27 Abs. 3 nur in Übereinstimmung mit entsprechenden gesetzlichen Regelungen zulässig. Eine Datenübermittlung und -verbreitung ist nach Art. 21 Abs. 1 ausgeschlossen, wenn sie für andere Zwecke erfolgen soll als diejenigen, die in der Meldung an die Kontrollstelle genannt worden sind. Sie sind weiterhin nach Abs. 2 ausgeschlossen, wenn sie Gegenstand einer Löschungsanordnung sind oder sie länger gespeichert werden als dies zur Zweckerfüllung erforderlich ist. Die Kontrollstelle kann nach Abs. 3 die Verbreitung von Daten an eine unbestimmte Zahl von Empfängern untersagen, wenn dies bestimmten wichtigen öffentlichen Interessen widerspricht.

Zur differenzierten Regelung im künftigen allgemeinen Datenschutzgesetz Japans: Danach wird die Weitergabe personenbezogener Daten grundsätzlich ausgeschlossen. Sie wird jedoch

---

597 S. Teil 3 Kap 3.1.

598 Gesetz Nr. 675 vom 31.12.1996.

599 S. hierzu auch das Widerspruchsrecht nach Art. 13 Abs. 1 e) – s. hierzu Kap. 6.4.

600 S. hierzu Kap. 3.3.1.1.

601 Als Teil der Datenverarbeitung ist die Übermittlung zulässig, wenn sie für die Vertragserfüllung erforderlich ist. Die Übermittlung oder Verbreitung ist nach Art. 21 Abs. 4 a) immer zulässig, wenn sie zu wissenschaftlichen Zwecken erforderlich ist.

602 Gesetz Nr. 675 vom 31.12.1996.

in mehreren Ausnahmen weitgehend ermöglicht, aber im Prinzip nur, wenn dies der betroffenen Person vorher angezeigt wurde und bei Datenverarbeitung zur Weitergabe an Dritte ihr ein Widerspruch ermöglicht wird.[603]

3.5.6 Zweckbindung, Auftragsdatenverarbeitung und Funktionsübertragung

Für die Auftragsdatenverarbeitung sollte im Wesentlichen die geltende Regelung[604] beibehalten werden. Allenfalls könnte erwogen werden, den Auftragnehmer gegenüber der betroffenen Person stärker in die Verantwortung für eine korrekte Datenverarbeitung zu nehmen. Zwar ist die Regelung richtig, dass gegenüber der betroffenen Person der Auftraggeber auch für die rechtsgemäße Datenverarbeitung des Auftragnehmers einstehen muss, da er ihn auswählt und anleitet. Da der Auftraggeber aber keine realistische Chance hat, die Datenverarbeitung beim Auftragnehmer tatsächlich zu überprüfen, faktisch also der Auftragnehmer Umfang und Form der Datenverarbeitung bestimmt, könnte erwogen werden, ihn gegenüber der betroffenen Person subsidiär für die Rechtmäßigkeit der Datenverarbeitung rechtlich verantwortlich zu machen. Eine solche direkte Haftung gegenüber dem Betroffenen erweitert die Kompensationschancen der betroffenen Person insbesondere dann, wenn die wirtschaftlichen Möglichkeiten des Auftraggebers begrenzt sind.

Für das Outsourcing der Datenverarbeitung an einen Dritten ist jedoch eine eigene Regelung notwendig. Im Unterschied zur Auftragsdatenverarbeitung, bei der dem Auftragnehmer nur eine Hilfsfunktion übertragen wird und der Auftraggeber die volle und alleinige Verantwortung für die Datenverarbeitung behält, wird bei der Funktionsübertragung die Aufgabe mit der Datenverarbeitung vollständig auf einen Dritten übertragen, der die Datenverarbeitung in eigener Verantwortung durchführt.[605] Beispiele hierfür sind die Übertragung der Personaldatenverarbeitung in einem Konzern an ein eigens hierfür gegründetes Tochterunternehmen, die Übertragung von Anwaltsforderungen an ein Inkassounternehmen, die Abrechnung von Arztleistungen durch eine privatärztliche Verrechnungsstelle, die Übertragung von Sicherungsaufgaben an einen Wachdienst oder die Übertragung von Marketingaufgaben an ein selbständiges Marketingunternehmen. Die Weitergabe der zur Aufgabenerfüllung erforderlichen Daten ist eine Datenübermittlung an einen Dritten und daher nach dem hier vorgeschlagenen Konzept nur zulässig, wenn sie von einer Einwilligung oder einem Erlaubnistatbestand[606] gedeckt ist und die Voraussetzungen für eine Ausnahme von der grundsätzlichen Pflicht, die Daten bei der betroffenen Person zu erheben,[607] vorliegen.[608] Die Möglichkeit der Funktionsübertragung wird durch diese Zulässigkeitsvoraussetzungen gegenüber der heute weit verbreiteten Praxis eingeschränkt werden.

Die Funktionsübertragung ist als eine Form des Outsourcing aus organisatorischen, technischen und wirtschaftlichen Gründen, aber auch zur besseren Gewährleistung der Datensicherheit oft sinnvoll und sollte nicht behindert werden. Andererseits darf sie nicht dazu genutzt werden können, die Verantwortung für eine Datenverarbeitung im eigenen Interesse und lästige Datenschutzpflichten zu Lasten der betroffenen Person auf andere abzuschieben. Um die Datenübermittlung im Rahmen der Funktionsübertragung zu ermöglichen, zugleich aber den Missbrauch dieser Organisationsform der Datenverarbeitung zu verhindern, sollte für die Datenübertragung im Rahmen einer Funktionsübertragung folgende Regelung gelten:

---

603 Zur differenzierten Regelung s. japanische Expertenkommission 2000, 8.

604 S. § 11 BDSG, Art. 17 DSRL.

605 S. hierzu z.B. *Tinnefeld/Ehmann* 1998, 245; *Walz*, in: *Simitis u.a.*, BDSG, § 11 Rn. 18 ff.; *Breidenbach* 1999.

606 S. Teil 3 Kap. 3.1.4.

607 S. Teil 3 Kap. 3.2.2.

608 S. Teil 3 Kap. 3.5.5.

Die Übermittlung sollte im Rahmen der Funktionsübertragung erleichtert werden, indem sie grundsätzlich als von einer Einwilligung oder einem Vertrag mit der datenerhebenden Stelle gedeckt angesehen werden kann, wenn die betroffene Person zuvor von dieser Zweckänderung informiert worden ist.[609] Ihr soll damit die Möglichkeit eingeräumt werden, der Weitergabe ihrer Daten zu widersprechen. Sofern die datenerhebende Stelle ihre gesamte Datenverarbeitung ausgelagert hat, wird der Widerspruch allerdings nur befolgt werden können, indem das Vertragsverhältnis mit der betroffenen Person beendet wird. Diese Erleichterung der Übermittlung ist allerdings nur vertretbar, wenn durch die Funktionsübertragung der Schutz der Daten oder die Rechtsstellung der betroffenen Person nicht beeinträchtigt werden. Um beides zu erreichen, ist die Zulässigkeit der Funktionsübertragung mit Sicherungen für die betroffene Person zu verbinden: Die übermittelnde Stelle darf nicht völlig aus der datenschutzrechtlichen Verantwortung entlassen werden und beim Funktionsübernehmer müssen vergleichbare rechtliche und tatsächliche Bedingungen geschaffen werden, wie sie die übermittelnde Stelle bei eigener Datenverarbeitung bieten müsste. Eine Übermittlung im Rahmen der Funktionsübertragung sollte dann als zulässige Datenverarbeitung angesehen werden, wenn die folgenden Voraussetzungen erfüllt sind:

Die übermittelnde Stelle, die Daten über die betroffene Person erhebt, aber von anderen in ihrem Interesse verarbeiten lässt,[610] bleibt weiterhin verantwortlich und hat für die Rechtmäßigkeit der Datenverarbeitung und für die Erfüllung der Betroffenenrechte einzustehen. Sie muss vor allem sicherstellen, dass die für sie geltende Zweckbindung auch für die Datenverarbeitung beim Funktionsübernehmer gilt. Die übermittelnde Stelle hat in einem Funktionsübertragungsvertrag entsprechende Vereinbarungen zu treffen. Eine ähnliche Regelung enthalten für die Auslagerung der Abrechnung bei Telekommunikations- und Telediensten bereits § 7 Abs. 1 TDSV, § 6 Abs. 4 TDDSG und § 15 Abs. 4 MDStV.

Der Funktionsübernehmer ist ebenfalls verantwortliche Stelle und hat deren Pflichten zu erfüllen. Im Funktionsübertragungsvertrag sind intern die Weisungs- und Verantwortungsbereiche abzugrenzen. Die betroffene Person kann ihre Datenschutzrechte auch gegenüber dem Funktionsübernehmer geltend machen. Auch für ihn gilt die gleiche Zweckbindung der Daten wie für die übermittelnde Stelle, ebenso die gleichen Sicherungs- und Geheimhaltungspflichten.[611]

Um ein Outsourcing (sowohl Auftragsdatenverarbeitung als auch Funktionsübertragung) durch Ärzte, Rechtsanwälte, Versicherungen und andere Geheimnisträger überhaupt rechtlich zu ermöglichen, sollte die Strafvorschrift des § 203 StGB auf die Auftrag- und Funktionsübernehmer erstreckt werden. Nur wenn die Daten beim Auftrag- und Funktionsübernehmer zu den gleichen rechtlichen Bedingungen wie beim Geheimhaltungspflichtigen verarbeitet werden, ist eine Übermittlung – wenn sie nicht aus sonstigen rechtlichen Gründen ausgeschlossen ist – vertretbar. Der Auftrag- oder Funktionsübernehmer sollte in bezug auf bestimmte Daten, die er von einem Arzt, Rechtsanwalt oder einem anderen Geheimnisträger erhalten hat, die gleichen Zeugnisverweigerungsrechte und den gleichen Beschlagnahmeschutz haben, wie derjenige, für den oder in dessen Interesse er diese Daten verarbeitet. Sie sind durch das Outsourcing der Datenverarbeitung nicht weniger schutzwürdig.

---

609 Dies ist nicht notwendig, wenn die Datenübermittlung im Rahmen der Funktionsübertragung bereits Gegenstand der Einwilligung oder der Vertragsabsprachen war.

610 Da Übermittlungen oft im beiderseitigen Interesse stattfinden, wird eine Abgrenzung zwischen einer Datenübermittlung außerhalb und innerhalb einer Funktionsübertragung nicht immer einfach sein. In der Praxis dürfte sich die Abgrenzung oft dadurch erübrigen, dass derjenige, der die erleichterte Übermittlung im Rahmen der Funktionsübertragung in Anspruch nimmt, damit zum Ausdruck bringt, dass es sich um eine Funktionsübertragung und nicht um eine sonstige Datenübermittlung handelt.

611 S. z.B. *Vogt/Tauss* 1998, Nr. 15; *Jandach*, DuD 2001, 224.

Ein Outsourcing kann unter diesen Umständen zu einer Verbesserung des Datenschutzes und der Datensicherung führen. Die Daten sind beim Dienstleister unter Umständen sicherer und besser aufgehoben, als in der einzelnen Arztpraxis, in der niemand sich für Datenschutzprobleme interessiert und sich mit Datenverarbeitungssystemen und ihrer Sicherung auskennt.

Das schweizerische Bundesgesetz über den Datenschutz[612] erlaubt in Art. 14, die Datenverarbeitung einem Dritten zu übertragen, wenn der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet.

3.5.7 Technisch-organisatorische Sicherung der Zweckbindung

Neben der Vermeidung und Minimierung personenbezogener Daten *(Datenvermeidung und Datensparsamkeit)* ist die technisch-organisatorische Sicherung der Zweckbindung die zweite wichtige Aufgabe des Systemdatenschutzes: Grundsätzlich sollten die verwendeten Produkte und die eingerichteten Datenverarbeitungsprozesse für die verarbeitenden Personen nur die Maßnahmen zulassen, die dem Zweck der Datenverarbeitung entsprechen.

Dieses Ziel muss unter anderem durch folgende Maßnahmen zu erreichen versucht werden:

(1) Durch organisatorische Maßnahmen, die technisch unterstützt werden können, soll sichergestellt werden, dass Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt verarbeitet werden. Eine „informationelle Gewaltenteilung" soll verhindern, dass Daten aus unterschiedlichen Zusammenhängen und Entstehungsgründen zusammengeführt werden. Die Chance eigener Selbstdarstellung in unterschiedlichen Kommunikationsbeziehungen soll dadurch sichergestellt werden, dass Daten aus unterschiedlichen Lebensbereichen und sozialen Beziehungen getrennt gehalten werden.[613]

Diese Anforderung, die in Nr. 8 der Anlage zu § 9 BDSG neu aufgenommen worden ist, zielt wie ihr Vorbild, das Gebot der getrennten Verarbeitung von Daten über die Inanspruchnahme verschiedener Tele- und Mediendienste in § 4 Abs. 2 Nr. 4 TDDSG und § 13 Abs. 2 Nr. 4 MDStV, darauf, die Zusammenführung von personenbezogenen Daten zu Persönlichkeitsprofilen zu verhindern. Das Trennungsgebot verbietet auch die Verarbeitung heterogener personenbezogener Datenbestände in sogenannten Data Warehouses, in denen Daten zur späteren Nutzung zu noch nicht festgelegten Zwecken auf Vorrat gehalten[614] und unter Verwendung von Methoden des Data-Mining ausgewertet werden sollen.[615] Die Datenverarbeitungstechnik muss zumindest technisch ermöglichen, dass die Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt verarbeitet werden können. Sie sollen nicht aus technischen Gründen zusammengeführt werden müssen.

Eine wirksame Form informationeller Gewaltenteilung ist es, das Erbringen einer Funktion so auf mehrere Instanzen (seien es Organisationen, seien es Geräte) zu verteilen, dass diese nur gemeinsam die Funktion erbringen können, einzelne Instanzen aber allein keinen Schaden verursachen können, also etwa die Datenverarbeitung verhindern oder verfälschen, personenbezogene Daten unbefugt auswerten oder weitergeben. Bei vielen heutigen Informations- und Kommunikationssystemen ist dies wegen der Befürchtung eines hohen Aufwands noch nicht realisiert. Da aber die Kosten der Informations- und Kommunikationstechnik bezogen auf ihre

---

612 Gesetz vom 19.6.1992 (Stand. 7.7.1998).

613 S. *v. Zezschwitz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.1, Rn. 1.

614 *Möller*, DANA 3/1998.

615 S. näher *Scholz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 9.2. *Möncke*, DuD 1998, 561; *Bizer*, DuD 1998, 570; *Baeriswyl*, RDV 2000, 6; *Büllesbach*, CR 2000, 11; *59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder* (Entschließung vom 14./15. März 2000): Data Warehouse, Data Mining und Datenschutz, RDV 2000, 138 = http://www.datenschutz-berlin.de/doc/de/ konf/59/datawa.htm.

Leistungsfähigkeit drastisch abnehmen[616] und sich dieser Trend mindestens noch in den nächsten zehn Jahren fortsetzen wird, sollte eine solche technische Unterstützung der informationellen Gewaltenteilung zunehmend angestrebt werden. Eine Zielfestlegung der Bundesregierung könnte hierfür das geeignete Instrument sein.[617]

(2) In Ergänzung zur getrennten Datenverarbeitung fordert das Bundesverfassungsgericht zur Sicherung der Zweckbindung, dass eine zweckgebundene Abschottung der erhobenen Daten erfolgt.[618] Der Zweckbindung dienen auch Maßnahmen zur Zugangs-, Zugriffs- und Weitergabekontrolle, wie sie von der Anlage zu § 9 BDSG gefordert werden. Schutz der Zweckbindung gegenüber Unbefugten kann auch durch Verschlüsselung bewirkt werden. In offenen Netzen wie dem Internet kann sie nur durch Kryptographie sichergestellt werden. Wenn es nicht möglich ist, Unbefugte am Zugriff auf die Daten zu hindern, so kann doch durch kryptographische Verschlüsselung verhindert werden, dass das Zugreifbare interpretiert und damit missbräuchlich verwendet werden kann.[619] In § 6 LDSG Schleswig-Holstein wird unter anderem zur Zwecksicherung gefordert, dass die personenbezogenen Daten verschlüsselt sein müssen, wenn sie außerhalb der eigenen Räume der datenverarbeitenden Stelle verarbeitet werden. Verschlüsselung wird auch durch § 13 Transplantationsgesetz (TPG) und § 6 und 7 Krebsregistergesetz (KRG) gefordert.[620] Diese Regelungen sollten zum Vorbild genommen und die Forderung nach Verschlüsselung in das allgemeine Datenschutzgesetz übernommen werden.[621]

Personenbezogene Daten sollten weder unverschlüsselt gespeichert noch dürfen sie unverschlüsselt übertragen werden. Heutige Speichermedien können erfolgreich entwendet und gelesen werden – sie sind klein, leicht und standardisiert, Kommunikationsnetze können leicht abgehört werden – bei vielen Netzen, insbesondere allen, die mit Broadcast arbeiten, wie dies LANs oder Funknetze tun, ist dies im buchstäblichen Sinne kinderleicht.

Bei der Auswahl von Verschlüsselungsverfahren ist darauf zu achten, dass zuverlässige, sichere Verfahren verwendet werden, deren Details offengelegt sind und die von der Scientific Community seit mindestens fünf Jahren intensiv untersucht worden sind. Diese Verfahren sollten keine Möglichkeit bieten, im Bedarfsfall eine Entschlüsselung und damit die Rekonstruktion des Klartexts zu ermöglichen. Dies liefe dem Anliegen der Verschlüsselung zuwider, da deren Missbrauch vorherbestimmt wäre.[622] Ohne Ausnahme gilt, dass eine Rekonstruktion von Schlüssel oder Klartext bei der Übertragung von Nachrichten nie nötig ist: Es ist immer leichter und für den Schutz der personenbezogenen Daten ungefährlicher, den Sender um eine nochmalige, mit einem neuen Schlüssel verschlüsselte Übertragung zu bitten. Eine Rekonstruktion von Schlüsseln oder Klartexten darf allenfalls nur bei längerfristig gespeicherten Daten vorgesehen werden.[623]

(3) Das Bundesverfassungsgericht fordert eine Kennzeichnung des Zwecks der erhobenen Daten, um kontrollieren zu können, wenn Daten, die nur zu einem besonderen Zweck erhoben

---

616 S. Teil 1 Kap. 2.2 sowie Anhang 1, S. 224 ff.

617 S. hierzu Teil 3 Kap. 6.2.

618 *BVerfGE* 65, 1 (50).

619 S. auch *Heibey*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.5, Rn. 112.

620 S. hierzu *Kloepfer* 1998, D 98f.

621 S. Teil 3 Kap. 3.5.8.

622 Eine Rekonstruktionsmöglichkeit selbst nur für ausgewählte Instanzen vorzusehen, die entweder den verwendeten Schlüssel (Key Recovery) öffnen oder ohne vorherige Entschlüsselung den Klartext selbst rekonstruieren können (Message Recovery), wäre ebenso kontraproduktiv, da sie allein auf dem Vertrauen in diese Instanzen (und ihr Equipment) aufbauen müsste.

623 S. hierzu *Huhn/Pfitzmann*, 1997, 500ff.

werden durften, zu anderen Zwecken verwendet werden.[624] Grundsätzlich können den Daten Kennzeichen des Zwecks ihrer Erhebung mitgegeben werden. Solche Zweckbindungs-Kennzeichen müssen durch entsprechende Hardware unterstützt werden. Ihre ungeschützte Speicherung könnte jedoch das Gegenteil des erwünschten Erfolgs, nämlich eine Schwächung des Datenschutzes nach sich ziehen: Die Zweckbindungs-Kennzeichen könnten dann beispielsweise von Data-Mining-Werkzeugen genutzt werden, um gezielt nach solchen Daten zu suchen und sie entgegen der Zweckbindung zu interpretieren und zu nutzen. Deshalb sollten Zweckbindungs-Kennzeichen von der Anwendungssoftware nicht unmittelbar gelesen werden können, sondern nur unter einer zweckbezogenen Kontrolle des Betriebssystems. Eine technische Realisierungsmöglichkeit besteht in einer *tagged architecture*, bei der das Betriebssystem die Anwendungssoftware beim Zugriff auf diese Kennzeichen (*tags*) strikt kontrolliert.[625]

Die Umsetzung der Forderung des Bundesverfassungsgerichts stößt allerdings auf mehrere Schwierigkeiten: Zwar ließe sich zum Einen den personenbezogenen Daten jeweils der Zweck ihrer Erhebung und gegebenenfalls Verarbeitung und Übermittlung in einem Beschreibungsfeld beifügen. Auch wäre der informations- und kommunikationstechnische Aufwand hierfür hinsichtlich Prozessorleistung und Speicherplatz nicht hoch. Der Programmieraufwand dürfte allerdings erheblich sein, wenn bestehende Systeme geändert werden müssten, ebenso der Umstellungsaufwand für organisatorische Verfahren. Zum Anderen setzt eine *tagged architecture* ein neues Betriebssystem voraus, das erst noch entwickelt werden müsste. Hierfür wäre – selbst wenn eine solche Entwicklung öffentlich gefördert würde – ein Zeitraum von etwa zehn Jahren erforderlich. Es wird empfohlen, Forschungs- und Entwicklungsprojekte zu initiieren und zu finanzieren, die die Tragfähigkeit dieser Idee für den Datenschutz untersuchen und Prototypen entwickeln. Inhalt der Untersuchungen sollte auch sein, wie sich solche *tagged architectures* auf die Rechte von Betroffenen (Transparenz, Auskunft) oder auf die Möglichkeiten der Prüfung durch Kontrollstellen oder (interne) Datenschutzbeauftragte auswirken. Erst danach kann über ihre Einführung entschieden sowie gegebenenfalls eine Einführungsstrategie festgelegt werden.

Bis dahin könnte die Forderung des Bundesverfassungsgerichts rechtlich eingefordert und durch Strafbewehrung abgesichert werden. Eine solche Forderung wäre – trotz fehlender technischer Sicherung – nicht folgenlos. Denn es dürfte nicht einfach sein, nachträglich das Zweckkennzeichen zu bestimmten Daten perfekt zu fälschen. In der Regel gibt es immer ein Protokoll, einen Ausdruck oder sonst eine Unterlage, die den alten Zustand belegen. Verbunden mit einer Strafandrohung könnten, angesichts des damit einher gehenden Risikos, zumindest Routinen mit unerlaubter Zweckänderung verhindert werden.

Doch auch diese Lösung stößt auf das Problem, dass die Kennzeichnung der Zwecke derzeit in keiner Datenbank vorgesehen ist. Die Forderung, alle Datenbanken nachzurüsten, um bei jedem Datum ein Feld für die Zwecke der Verarbeitung vorzusehen, würde für die verantwortlichen Stellen hohe Kosten verursachen und wäre daher bezogen auf den (begrenzten, weil nicht technisch abgesicherten) Vorteil für den Datenschutz wohl nicht verhältnismäßig. Die Forderung könnte somit allenfalls nach einer längeren Übergangsfrist umgesetzt werden. Sie sollte Gegenstand einer Zielfestlegung der Bundesregierung sein.[626]

---

624 *BVerfGE* 100, 313 (360f.).

625 Solche *tagged architectures* gab es schon einmal – allerdings beschrieben die *tags* nicht Zwecke, sondern Datentypen des Rechners wie Integer, Gleitkommazahlen, Pointer etc..

626 S. zu diesem Instrument Teil 3 Kap. 6.2.

3.6 Datensicherung

Die verantwortliche Stelle hat die erhobenen Daten ausreichend durch technisch-organisatorische Maßnahmen so zu sichern, dass Risiken für die informationelle Selbstbestimmung vermieden werden.

Die in der Anlage zu § 9 BDSG geregelten „acht Gebote" der technischen und organisatorischen Maßnahmen bedürfen einer grundsätzlichen Reform. Insbesondere sind in einem modernisierten BDSG auch die Schutzziele der Informationstechnik zum Datenschutz aufzunehmen. Die Regelung von Schutzzielen und Maßnahmen im BDSG sollte wie folgt erfolgen:

Zum Einen sollten sie jeweils dort genannt werden, wo die zugehörigen rechtlichen Schutzziele beschrieben werden. Beispiele hierfür sind Begriffe wie „Anonymität" oder „Pseudonymität", die schon allein durch den Begriff selbst nahelegen, dass – sofern nicht die gegenstandsweltliche Anwendung selbst bereits dafür sorgt – im IT-System entsprechende informationstechnische Mechanismen implementiert sind, die Anonymität und Pseudonymität gegenüber jedermann von Beginn an gewährleisten. Die Verankerung erfolgt hier, indem nicht wie in § 3 Abs. 6 und 6a BDSG die Begriffe „Anonymisieren" oder „Pseudonymisieren" gewählt werden, die unterstellen, dass es außer der betroffenen Person noch mindestens eine weitere Instanz gibt, die ihre Identität kennt und erst nachträglich anonymisiert oder pseudonymisiert. Um zusätzliche Klarheit zu schaffen, bieten sich vielmehr Definitionen dieser Begriffe an, die so geschrieben sind, dass sie entsprechende Schutzziele und Maßnahmen der Informationstechnik nahelegen.[627]

Zum Anderen werden die Schutzziele und Maßnahmen der Informationstechnik zum Datenschutz in einem oder wenigen Paragraphen gebündelt beschrieben, um die technisch-organisatorischen Anforderungen zusammenhängend zur Kenntnis nehmen zu können.

Bezogen auf die Detaillierung der Regelung sollte angestrebt werden, sich im Wesentlichen auf Schutzziele der Informationstechnik zu beschränken. Ergänzend können im Einzelfall, wo dies sinnvoll und hilfreich erscheint, auch beispielhafte Maßnahmen zur Umsetzung der Schutzziele genannt werden.[628] Die Definition von Schutzzielen ist der Benennung allein von Maßnahmen vorzuziehen, da diese insbesondere technologieunabhängig zu definieren sind und einen allgemeingültigen Sicherheitsrahmen bilden, der umfassend ist und auch bei neuen Formen der Datenverarbeitung Bestand haben wird.

Als *grundlegende Schutzziele der Informationstechnik in Bezug auf die Verarbeitung personenbezogener Daten* können betrachtet werden:

Datensparsamkeit: Informationstechnische Systeme sind so zu gestalten, dass keine personenbezogenen oder -beziehbare Daten oder so wenige wie möglich anfallen. Grundsätzlich ist die Erfassungs*möglichkeit* personenbezogener oder -beziehbarer Daten zu vermeiden. Wo dies nicht möglich oder unverhältnismäßig zum angestrebten Schutzzweck ist, sind die Erfassung, wo dies nicht möglich oder unverhältnismäßig ist, die Verarbeitung und Speicherung in ihrem Umfang wie in ihrer Dauer zu minimieren.[629]

Vertraulichkeit: Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.

---

627 S. die Definitionen von Anonymität und Pseudonymität in Teil 3 Kap. 3.4.3.

628 Dies entspricht auch dem Votum des Arbeitskreises „Technische und organisatorischen Fragen des Datenschutzes" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 2./3. März 1999 –s. http://www.datenschutz-berlin.de/to/blaend.htm.

629 S. hierzu bereits Teil 3 Kap. 3.4.1.

Integrität: Personenbezogene Daten bleiben während der Verarbeitung unverfälscht und vollständig oder es ist mit sehr großer Wahrscheinlichkeit klar erkennbar, dass dies nicht der Fall ist. Diese sogenannte *innere* Integrität kann in IT-Systemen durch Maßnahmen der Informationstechnik gewährleistet werden. Nicht allein durch Maßnahmen der Informationstechnik zu gewährleisten ist die sogenannte *äußere* Integrität, die sich auch auf die Aktualität der personenbezogenen Daten bezieht.

Verfügbarkeit: Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden.

Zurechenbarkeit: Personenbezogene Daten können ihrem Ursprung jederzeit zugeordnet werden.

Revisionsfähigkeit: Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Transparenz: Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können.

Die Ziele Datensparsamkeit und Revisionsfähigkeit stehen scheinbar im Widerspruch zueinander. Bei genauerer Betrachtung ist dieser Widerspruch jedoch auflösbar: Während Revisionsfähigkeit mehr Datensammlung und beweisgeeignete Speicherung auf der Meta-Ebene der Datenverarbeitung erfordert, bezieht sich Datensparsamkeit auf die konkrete Ebene der personenbezogenen Daten.

Die Erfüllung der Schutzziele sollte nach dem jeweiligen Stand der Technik erfolgen. Die bisherige Lösung im BDSG (Anlage zu § 9) hat sich entgegen der guten Absicht von 1976 als ziemlich starr erwiesen. Mit dem Verweis auf den Stand der Technik wird ein dynamischer Maßstab für die Erfüllung der Schutzziele eingeführt. Er orientiert sich an den fortschrittlichen Verfahren, die sich mit Erfolg im Betrieb bewährt haben. Der jeweilige Stand der Technik wird vielfach in einschlägigen Normen und in der Fachliteratur dokumentiert. Ein Beispiel ist das Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Die Wahl der Maßnahmen hat sich außer am Stand der Technik an einer Risikobewertung im Rahmen von Sicherheitskonzepten[630] zu orientieren. Die Angemessenheit ist auf der Grundlage von Risikoanalysen zu konkretisieren. Wo dies angemessen ist, insbesondere bei Maßnahmen, die gegen unterschiedlich starke Angreifer wirksam sind, ist eine klare Priorisierung von Schutzzielen und Maßnahmen durchzuführen.

4. Datenschutzmanagement

Die Umsetzung der dargestellten Grundsätze der Datenverarbeitung muss durch organisatorische Datenschutzmaßnahmen der verantwortlichen Stelle gewährleistet und unterstützt werden.

4.1 Datenschutzmanagementsystem

Um Verantwortlichkeit sicher zu stellen, das Datenschutzbewusstsein zu stärken und eine datenschutzfördernde Betriebsorganisation zu erreichen, sollte nach dem Vorbild des Umweltschutzrechts der Aufbau von Datenschutzmanagementstrukturen gefördert werden. Hierzu sollen viele bereits bestehende organisatorische Verpflichtungen der verantwortlichen Stellen zusammengefasst und zu einem integrierten Datenschutzmanagementsystem fortent-

[630] S. im Folgenden Kap. 4.1.

wickelt werden. Dies soll vor allem dadurch geschehen, dass verantwortliche Stellen, die verpflichtet sind, einen Datenschutzbeauftragten zu bestellen,

- einen Plan der Datenschutzorganisation erarbeiten und
- ein Datenschutz- und Datensicherheitskonzept erstellen.

Aus dem *Datenschutzorganisationsplan* soll sich eindeutig ergeben, wer für welche Aufgaben des Datenschutzes verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit des Plans trägt.[631] In ihm ist auch verbindlich und revisionssicher festzulegen, wer über welche Befugnisse bei der Verarbeitung personenbezogener Daten verfügt. Diese Festlegungen verhindern, dass Verantwortung für bestimmte Verarbeitungsschritte nicht zugeordnet und eingefordert werden kann. Nur mit Hilfe dieser Angaben können Kontrollen befugte und unbefugte Personen unterscheiden und deren Handeln überprüfen.[632] Der Organisationsplan sollte auch eine Festlegung enthalten, wer für die verantwortliche Stelle Verfahren der automatisierten Datenverarbeitung freigibt. Um die Wahrnehmung seiner Verantwortung sicher zu stellen, sollte dies der Leiter der verantwortlichen Stelle oder ein Mitglied des Leitungsgremiums sein. Schließlich ist auch festzulegen, wer dafür verantwortlich ist, dass notwendige Dokumentationen rechtzeitig erstellt und korrekt aufbewahrt werden und dass die Beschäftigten systematisch in der Praxis des Datenschutzes unterwiesen werden.

Das *Datenschutz- und Datensicherheitskonzept* sollte ein wesentliches Ergebnis der Vorabkontrolle sein, sofern diese durchgeführt wird. Die in Art. 20 DSRL und § 4d Abs. 5 und 6 BDSG enthaltene Verpflichtung, bei Datenverarbeitungen mit spezifischen Risiken vor deren Beginn eine Prüfung der Datenverarbeitung durchzuführen, ist beizubehalten.[633] Sie sollte in Form einer Technikfolgenabschätzung erfolgen, wie sie zum Beispiel § 7 Abs. 3 LDSG Niedersachsen[634] und § 20 BDSG-Entwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN[635] vorsieht.

Bestandteile des Datenschutz- und Datensicherheitskonzepts sollten sein:

- Die nach § 4e Abs. 1 Nr. 1 bis 8 BDSG meldepflichtigen Angaben. Diese enthalten die Basisinformationen über die Datenverarbeitung. Zu beschreiben ist darüber hinaus der Aufbau der Datenverarbeitungssysteme und die personellen oder programmgesteuerten Abläufe bei der Datenverarbeitung.
- Eine Darstellung, wie die Grundsätze zur Datenverarbeitung eingehalten werden. Hierzu gehört, wie sichergestellt wird, dass die betroffenen Personen unterrichtet werden, die Datenschutzerklärung erstellt und fortgeschrieben wird, die Erforderlichkeitsprüfung durchgeführt[636] und die Zweckbindung gewährleistet wird. Zu beschreiben ist auch, wie die Erfüllung der Ansprüche betroffener Personen gewährleistet und insbesondere sichergestellt wird, dass Berichtigungen, Sperrungen und Löschungen, Einwände, Anonymisierungen und Pseudonymisierungen an alle Empfänger der Daten nachgemeldet werden können.[637] Hierzu gehört auch eine Darstellung, wie die Einhaltung der Verarbeitungs-

631 S. hierzu das Vorbild des 52a BImSchG.

632 S. *Heibey*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.5, Rn. 89

633 S. hierzu z.B. *Klug*, RDV 2001, 12; *Schild*, DuD 2001, 282.

634 S. hierzu *Hube*, DuD 1999, 31.

635 BT-Drs. 13/9082.

636 Hierzu gehört auch die Festlegung konkreter Prüf- und Löschungsfristen und Maßnahmen zu ihrer Durchsetzung – s. Teil 3 Kap. 3.4.1.

637 S. hierzu Kap. 3.2.3.

grundsätze durch organisatorische Vorkehrungen und die Sanktionierung von Verstößen sichergestellt wird.[638]

- Eine Darstellung, wie die Zielbestimmungen des Gesetzes[639] umgesetzt wurden oder warum keine weiteren Verbesserungen zu erzielen sind. In diesem Zusammenhang ist auch darzustellen, welche zertifizierten Produkte eingesetzt und warum verfügbare zertifizierte Produkte nicht eingesetzt werden.
- Eine Festlegung der konkreten Aufgaben und Befugnisse des Datenschutzbeauftragten einschließlich des Verfahrens bei Beschwerden betroffener Personen.[640]
- Eine Beschreibung, wie die Beobachtung der technischen Entwicklung und ihrer Auswirkungen auf die Risiken für die informationelle Selbstbestimmung und die Möglichkeiten, sie zu schützen, sichergestellt wird. Diese Beobachtungspflicht betrifft insbesondere die wissenschaftlich-technischen Möglichkeiten, anonyme oder pseudonyme Daten zu reidentifizieren.
- Ein Sicherheitskonzept,[641] das eine Risikoanalyse, eine Schutzzweckbeschreibung, die Beschreibung der Maßnahmen zum technisch-organisatorischen Datenschutz und zur Gewährleistung der informationstechnischen Sicherheit[642] sowie eine Beschreibung und Bewertung der verbleibenden Risiken umfasst.[643] Für die Erstellung des Sicherheitskonzepts kann auf das IT-Sicherheitshandbuch und das IT-Grundschutzhandbuch des Bundesamts für die Sicherheit in der Informationstechnik (BSI) zurückgegriffen werden.

Organisationsplan und Datenschutzkonzept müssen bereitgehalten (oder der Kontrollstelle übergeben werden) und der Kontrollstelle bei Kontrollen übergeben werden.[644]

4.2 Datenschutzaudit

Mit einem Datenschutzaudit sollten marktgerechte Anreize zu einer Mobilisierung der Selbstverantwortung der verantwortlichen Stellen geschaffen werden. Zielsetzung des Datenschutzaudits ist die freiwillige Überprüfung des Datenschutzmanagementsystems[645] hinsichtlich seiner Eignung, eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit

---

638 Dies fordert auch FAQ 7 der häufig gestellten Fragen (FAQ), Anhang zu den Grundsätzen des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 16.

639 S. z.B. das Ziel, Auswahl und Gestaltung der Datenverarbeitungsprozesse und -systeme an dem Gebot der Vermeidung personenbezogener Daten auszurichten – Teil 3 Kap. 7.1.3, das Ziel, Verfahren einzusetzen, die anonymes und pseudonymes Handeln erlauben – Teil 3 Kap. 7.1.3, oder das Ziel, Online-Einsicht in die zu einer Person gespeicherten Daten zu gewähren – Teil 3 Kap. 7.1.3, Systeme mit offengelegtem Quellcode zu verwenden - s. Teil 3 Kap. 3.2.6.

640 S.. Teil 3 Kap. 7.2.

641 Ein solches wird bereits von § 87 Abs. 2 TKG und § 5 Abs. 3 LDSG SH gefordert.

642 S. *Heibey*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 4.5, Rn. 92.

643 S. hierzu auch *Ernestus*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 3.2.

644 S. das Vorbild in § 11 StörfallV; s. auch FAQ 7 der häufig gestellten Fragen (FAQ), Anhang zu den Grundsätzen des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG ABl. L 215 vom 25.8.2000, 16.

645 S. Teil 3 Kap. 4.1.

zu erreichen.[646] Es belohnt den Teilnehmer mit der abgesicherten Möglichkeit, im Wettbewerb um das Vertrauen der Kunden ein Auditzeichen zu führen, das die von einem zugelassenen Datenschutzgutachter überprüften Datenschutzanstrengungen bestätigt. Ergänzend zu den bestehenden Datenschutzregelungen sollen durch freiwillige Selbstregulation der Wirtschaftseinheiten und durch die Kräfte des Wettbewerbs Verbesserungen des Datenschutzes und der Datensicherheit ohne Zwang erzielt werden.[647] Das Datenschutzaudit mobilisiert legitimen Eigennutz, um dadurch Beiträge zur Verwirklichung von Gemeinwohlzielen hervorzubringen.

Eine Programmnorm zum Datenschutzaudit enthielt erstmals 1997 § 17 MDStV. Danach wurden solche Programmnormen in mehrere Landesdatenschutzgesetze und 2001 in § 9a BDSG aufgenommen.[648] Ausführungsvorschriften wurden in Schleswig-Holstein für das Behördenaudit nach § 43 Abs. 2 LDSG Schleswig-Holstein erlassen.[649]

Im Datenschutzaudit soll die Fähigkeit der datenverarbeitenden Stelle überprüft und prämiert werden, flexibel auf die rasanten Veränderungen der Informations- und Kommunikationstechniken zu reagieren und die sich dadurch immer wieder neu stellenden Herausforderungen für den Datenschutz zu meistern. Daher zielt das Datenschutzaudit nicht auf die einmalige Evaluierung, sondern auf die Fähigkeit, immer wieder neue Lösungen zu generieren, und daher auf die kontinuierliche Verbesserung des Datenschutzmanagementsystems.[650]

Ziel der Prüfung ist es, das Datenschutzmanagement danach zu bewerten, ob es für das jeweilige Verfahren geeignet und effektiv ist, die Einhaltung des geltenden Datenschutzrechts sicherzustellen und eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit zu erreichen.[651] Sofern das optimale Niveau hinsichtlich Datenschutz und Datensicherheit schon erreicht ist, erstreckt sich die Prüfung darauf, ob die verantwortliche Stelle in der Lage ist, dieses Niveau zu halten.[652]

Die Prüfung verwendet also zwei Maßstäbe: einen objektiven, für alle gleichen Maßstab, nämlich die Erfüllung der Anforderungen des Datenschutzrechts, und einen subjektiven, nämlich eine Verbesserung der Anstrengungen zum Datenschutz, die über den objektiven Maßstab hinausgeht und die sich nach den individuellen Möglichkeiten der verantwortlichen Stelle bestimmt. Von der selbstverständlichen Verpflichtung zur Einhaltung der geltenden Rechtsvorschriften abgesehen, bestimmen die verantwortlichen Stellen die inhaltlichen Anforderungen des Datenschutzaudits in Form von Selbstverpflichtungen selbst. Das Gesetz

---

646 S. positiv zu einem Datenschutzaudit *Roßnagel*, DuD 1997, 505; *ders*., DuD 2000, 231; *ders*., DuD 2001, 154; *Vogt/Tauss* 1998, Nr. 17; *Arbeitskreis „Datenschutzbeauftrage" im Verband der Metallindustrie Baden-Württemberg (VMI)*, DuD 1999, 281; *Königshofen*, DuD 1999, 266; *ders*., DuD 2000, 357; *Bäumler*, DuD 2001, 252; *Dieckmann/Eitschberger/Eul/Schwarzhaupt/Wohlrab*, DuD 2001, i.E.; die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24.10.1997 und 12./13.10.2000 sowie die Stellungnahme der Konferenz zum Gutachtendesign, das diesem Gutachten voranging (s. Anlage); ablehnend *Drews/Kranz*, DuD 1998, 98; *dies*., DuD 2000, 226; *Gola*, RDV 2000, 93.

647 Zur Gesetzgebungskompetenz s. *Roßnagel* 2000c, 134; *Bizer*/*Petri*, DuD 2001, 97.

648 Zur Geschichte des Datenschutzaudits s. ausführlich *Roßnagel* 2000c, 6 ff.

649 Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH, Amtsblatt S.-H. 13/2001, 196; s. hierzu *Bäumler*, DuD 2001, 252.

650 S. hierzu näher *Roßnagel* 2000c, 6.

651 *Roßnagel* 2000c, 63 ff.

652 Hiermit wird dem Bedenken Rechnung getragen, dass der Datenschutz ab einem bestimmten Niveau nicht mehr zu steigern sei – s. *Dieckmann/Eitschberger/Eul/Schwarzhaupt/Wohlrab*, DuD 2001, i.E. Dieses Bedenken dürfte sich in der Praxis jedoch als rein theoretisch erweisen. Innerhalb des Auditzeitraums von drei Jahren werden sich bei jedem Verfahren, auch wenn es bereits ein optimales Niveau erreicht haben sollte, die Zielsetzung, das Anwendungsfeld, die Rahmenbedingungen oder die eingesetzten Systeme so verändert haben, dass es an die Datenschutzanforderungen neu angepasst werden muss.

fordert nur, dass diese Anstrengungen auf eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit gerichtet sein und den wirtschaftlich vertretbaren Einsatz der besten verfügbaren Technik vorsehen müssen. Mit diesen beiden subjektiven Kriterien soll die Zielgerechtigkeit der Selbstverpflichtungen gewährleistet und die Vergleichbarkeit der zusätzlichen Anstrengungen aller Teilnehmer ermöglicht werden. Welche Anforderungen sich daraus für die verantwortliche Stelle ergeben, bestimmt diese in eigener Verantwortung.[653] Es bietet sich an, Empfehlungen für Selbstverpflichtungen im Rahmen branchenbezogener Selbstregulierung zu erarbeiten.[654]

Während Anstrengungen zur Verbesserung des Datenschutzes und der Datensicherheit das Ziel des Datenschutzaudits sind, sollte es für die verantwortlichen Stellen mit möglichst wenig zusätzlichem Verwaltungsaufwand verbunden sein. Zugleich muss aber auch die erforderliche Zielgerechtigkeit des Verfahrens und der Kriterien, die notwendige Transparenz und Vergleichbarkeit der Prüfergebnisse sowie die Rechtssicherheit für die Werberegeln gewährleistet sein.[655] Für die Wahl des geeigneten Verfahrens kommt es vor allem darauf an, welche verantwortlichen Stellen als Zielgruppe angesehen werden. Von ihnen muss erwartet werden, dass sie das Angebot eines Datenschutzaudits annehmen und mit ihrem Vorbild andere Stellen nachziehen. Ab einer gewissen Zahl und Bedeutung der Teilnehmer wird dann der Wettbewerb auch weitere Stellen veranlassen, am Datenschutzaudit teilzunehmen. Wie auch beim Umweltschutzaudit ist diese Zielgruppe eher in den etablierten und größeren Unternehmen zu sehen als in Internet-Start-Up-Unternehmen. Sie haben sowohl das Interesse als auch die Kapazität, ein Audit durchzuführen. Außerdem haben sie die erforderliche wirtschaftliche Bedeutung, um für andere verantwortliche Stellen vorbildhaft zu wirken. Da diese verantwortlichen Stellen in der Regel bereits an Qualitäts- und Umweltschutzaudits nach internationalen Normen[656] teilnehmen, wird die Einführung des Datenschutzaudits erleichtert und sein Verwaltungsaufwand reduziert, wenn es an die in den Unternehmen bereits bestehenden Managementsysteme angepasst wird.[657]

Da es keine geeignete Technische Norm für ein Datenschutzaudit gibt, kann es nur durch gesetzliche Regelungen geschaffen werden.[658] Durch diese Regelungen, die sich auf Rahmenvorgaben beschränken, nimmt der Gesetzgeber seine Gewährleistungsverantwortung für den Datenschutz und die Datensicherheit wahr. Wenn der elektronische Geschäftsverkehr und die elektronische Verwaltung gefördert werden sollen, ist eine gesetzliche Rahmenregelung des Auditverfahrens notwendig. Wie ausländische Erfahrungen mit unregulierter Selbstregulierung zeigen,[659] ist diese nicht geeignet, in kurzer Frist das notwendige Vertrauen der betroffe-

---

653 Zu den Maßstäben des Datenschutzaudits näher *Roßnagel* 2000c, 84 ff.

654 S. das Beispiel des *Arbeitskreises Datenschutzaudit Multimedia*, DuD 1999, 285.

655 S. hierzu näher *Roßnagel* 2000c, 126 ff.

656 Z.B. ISO 9.001 zum Qualitätsmanagement und ISO 14.001 zum Umweltschutzmanagement; EG-Verordnung Nr. 1836/93 vom 29.6.1993 „über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung" – EG ABl. Nr. L 168/1, vollständig neu gefasst durch EG-Verordnung Nr. 761/2001 „über freiwillige Beteiligung von Organisationen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung (EMAS) vom 19.3.2001, EG ABl. L 114 vom 24.4.2001, 1.

657 S. hierzu näher *Roßnagel* 2000c, 130 ff.

658 Ein unveröffentlichter Gesetzentwurf ist von *Roßnagel* bereits 1999 für das Bundesministerium für Wirtschaft und Technologie erstellt worden. Das diesem zugrunde liegende Gutachten wurde in *Roßnagel* 2000c veröffentlicht. Für eine gesetzliche Regulierung z.B. auch *Vogt/Tauss* 1998, Nr. 17; Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24.10.1997 und 12./13.10.2000 sowie die Stellungnahme der Konferenz zum Gutachtendesign, das diesem Gutachten voranging (s. Anlage).

659 S. *U.S. Federal Trade Commission* 2000; *Schwartz*, Vanderbilt Law Review 52 (1999), 1611; *Westin* 1997; *Reidenberg*, Berkeley Technology Law Journal, 14 (1999), 781 ff.; *ders*., Texas Law Review 76 (1998), 553 ff.; *Roßnagel* 2000b, 385; *ders*., 2000c, 25 ff.; *Grimm/Roßnagel*, DuD 2000, 446 jeweils m.w.N.

nen Personen in die Datenschutzmaßnahmen der verantwortlichen Stellen zu erzeugen. Selbstregulierung muss ein wesentlicher Bestandteil des Datenschutzaudits sein.[660] Aber darauf zu warten, bis die interessierten Kreise es tatsächlich geschafft haben, sich ohne Rahmenvorgaben auf ein vertrauenswürdiges und Vertrauen gewinnendes Verfahren zu einigen, es etablieren und zu praktizieren, würde der Bundesrepublik Deutschland einen gewaltigen Wettbewerbsnachteil bescheren.[661]

Das Datenschutzaudit sollte daher am Vorbild[662] des erfolgreichen Umweltschutzaudits der Europäischen Gemeinschaft[663] orientiert werden.[664] Allerdings ist es nicht notwendig, das Datenschutzaudit ähnlich aufwendig zu gestalten und in gleicher Weise umfangreich zu regeln.[665] In einer auf das Wesentliche reduzierten Form sollte das Datenschutzaudit in fünf Schritten durchgeführt werden:[666]

1. Grundlage des Datenschutzaudits ist eine *Datenschutzpolitik*, in der sich die verantwortliche Stelle selbst verpflichtet, alle einschlägigen Datenschutzvorschriften einzuhalten und Datenschutz und Datensicherheit unter wirtschaftlich vertretbarem Einsatz der besten verfügbaren Technik kontinuierlich zu verbessern oder auf höchstem Stand zu erhalten.
2. Auf dieser Grundlage legt die verantwortliche Stelle in einem *Datenschutzprogramm* zur Umsetzung der Datenschutzpolitik konkrete Datenschutzziele fest und bestimmt mit welchen konkreten Maßnahmen innerhalb welcher Fristen sie diese im Rahmen ihres Datenschutzmanagementsystems für das jeweilige Verfahren umsetzen will.
3. In periodischen Abständen führt das Unternehmen selbst eine *Datenschutzprüfung* als systematische und dokumentierte Analyse durch, ob das Datenschutzmanagementsystem die Umsetzung der Datenschutzpolitik und des Datenschutzprogramms sicherstellt.
4. Anhand des schriftlichen Prüfergebnisses prüfen und bestätigen sowohl der behördliche oder betriebliche *Datenschutzbeauftragte* als auch ein zugelassener unabhängiger *Datenschutzgutachter*, dass die Anforderungen an ein Datenschutzaudit eingehalten werden.
5. Im Falle einer positiven Validierung durch beide Prüfer wird das Prüfergebnis veröffentlicht und an die zuständige Behörde zur *Registrierung* im Verzeichnis der am Datenschutzaudit teilnehmenden Unternehmen weitergeleitet.

Um die Kosten eines Datenschutzaudits in Grenzen zu halten, bietet es sich an, die Fachkompetenz im eigenen Unternehmen für die Durchführung des Audits zu nutzen. Vor allem drängt es sich auf, dem betrieblichen oder behördlichen Datenschutzbeauftragten hierbei eine zentrale Rolle einzuräumen. Denn zwischen seinen Aufgaben und denen des Datenschutzaudits be-

---

660 S. oben die selbstgesetzten Kriterien der Prüfung.

661 Dagegen geht Japan den Weg zu regulierten und mit öffentlichem Vertrauen ausgestatteten Auditverfahren s. *Roßnagel* 2000c, 31 ff. sowie *Roßnagel*, DuD 2001, 154 ff. m.w.N.

662 S. zum Verfahren des Umweltschutzaudits *Roßnagel* 2000c, 43 ff.

663 Durch die Novellierung wurde der wesentliche Inhalt des Umweltschutzaudits nach dem weltweiten Standard ISO 14.001 in das europäische Umweltschutzaudit integriert.

664 S. zu den positiven Erfahrungen mit dem regulierten Umweltschutzaudit s. Bericht der *Bundesregierung* über die Erfahrungen mit dem Vollzug des Umweltauditgesetzes (UAG), BT-Drs. 11127 sowie *Roßnagel* 2000c, 47 ff. m.w.N.

665 Das Umweltschutzaudit ist in der Europäischen Verordnung zum Umweltschutzaudit, im Umweltschutzauditgesetz und vier Verordnungen in insgesamt 83 Paragraphen und mehreren Anhängen geregelt.

666 Von dem Gesetzentwurf von *Roßnagel* aus dem Jahr 1999 unterscheidet sich der folgende Vorschlag vor allem dadurch, dass er die Regelungen zu einem Datenschutzmanagement voraussetzen und daher deutlich „schlanker" gehalten werden kann. Ähnlich ist auch das Verfahren des Behördenaudits nach Nr. 4 ff. der Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH.

stehen viele Parallelen. Das Unternehmen muss sich in seiner Datenschutzpolitik verpflichten, die einschlägigen Datenschutzvorschriften einzuhalten und den Datenschutz kontinuierlich zu verbessern. Dies sind auch zentrale Aufgaben des betrieblichen oder behördlichen Datenschutzbeauftragten. Viele Teilaufgaben, die er in diesem Rahmen zu erfüllen hat, können auch für die Vorbereitung des Audits und die interne Datenschutzprüfung genutzt werden.[667]

Aufgrund der Registrierung ist die verantwortliche Stelle berechtigt, eine *Teilnahmeerklärung* und ein *Datenschutzzeichen* für Werbezwecke zu nutzen. Dieses Logo kann sie für die Kommunikation mit der Öffentlichkeit, insbesondere für Vertrauenswerbung nutzen. Ein gesetzlich geschütztes Zeichen für die überprüfte Selbstverpflichtung zur Einhaltung aller rechtlichen Datenschutzanforderungen und zu weitergehenden Anstrengungen zur kontinuierlichen Verbesserung des Datenschutzes und der Datensicherheit bietet tatsächlich eine Grundlage, dem Unternehmen Vertrauen entgegenzubringen.[668]

Um das notwendige Vertrauen der Bürger in das Auditzeichen zu erreichen, sind wenige Rahmenregelungen notwendig, die eine Vergleichbarkeit der Prüfungen und die Vertrauenswürdigkeit der Ergebnisse sicherstellen:[669]

Gegenstand des Datenschutzaudits ist nicht die verantwortliche Stelle, sondern ein oder mehrere Verfahren.[670] Eine gesamte verantwortliche Stelle dürfte im Regelfall als Gegenstand eines Datenschutzaudits zu groß und zu komplex sein. Betreibt eine verantwortliche Stelle nur eines oder wenige Verfahren, kann das Audit auch alle diese Verfahren und damit die gesamte Tätigkeit der verantwortlichen Stelle umfassen. Ein Verfahren ist durch eine mehrere Komponenten übergreifende Zielsetzung – wie etwa Personaldaten- oder Patientendatenverwaltung, Telekommunikationsversorgung oder elektronischer Warenverkauf – bestimmt. Es ist ein diesem Ziel dienender Prozess, in dem technische und organisatorische Komponenten systematisch zusammenwirken und in dem personenbezogene Daten verarbeitet werden. Nicht entscheidend ist der technische Zweck der einzelnen technischen oder organisatorischen Komponenten, sondern die übergreifende Zielsetzung, die eine oder mehrere verantwortliche Stellen mit dem Zusammenwirken dieser Komponenten verfolgen. Ein Verfahren könnte beispielsweise ein Personalverarbeitungs- und -abrechnungssystem, ein Krankenhausinformationssystem, ein Telekommunikationssystem oder ein Teledienst sein. Entscheidend ist, dass durch die Bestimmung der Anwendung eine in sich geschlossene Struktur für die Erhebung, Verarbeitung und Verwendung personenbezogener Daten erfasst wird, innerhalb derer die spezifischen Datenschutzrisiken vollständig überprüft werden können. Dies erfordert unter Umständen eine integrierte Sicht der Verarbeitung personenbezogener Daten wie etwa die Zusammenschau der Maßnahmen der Anbahnung, des Abschlusses und der Abwicklung eines Vertrags unter der Gesamtzielsetzung des elektronischen Handels. Zum Verfahren einer bestimmten Dienstleistung können beispielsweise die Datenverarbeitungssysteme zum Marketing, zur Kundenverwaltung, zum Erbringen der Vertragsleistung, zur Abrechnung, zum Bezahlen und zur Quittungserstellung, zur Wartung und zur Auswertung der Kundenkontakte sowie ihre Schnittstellen und Kommunikationswege gehören. Ein Verfahren ist nicht auf den Einflussbereich einer verantwortlichen Stelle beschränkt, sondern kann von mehreren verantwortlichen Stellen betrieben werden. Ein Verfahren ist auch nicht auf das Hoheitsgebiet eines

667 S. hierzu *Roßnagel* 2000c, 105 ff.

668 S. hierzu *Roßnagel* 2000c, 96 ff. S. auch Nr. 9 der Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH.

669 Ebenso der Evaluationsbericht zum IuKDG der Bundesregierung, BT-Drs. 14/1191,14.

670 In dem Gesetzentwurf von *Roßnagel* 1999 und in *Roßnagel* 2000c, 69 ff., wurde der Gegenstand noch „Anwendung“ genannt. Entsprechend dem Sprachgebrauch der Nr. 2 der Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH wird der Gegenstand des Datenschutzaudits „Verfahren“ genannt.

Staats beschränkt. Es kann grenzüberschreitend betrieben werden. Zum Verfahren gehört in jedem Fall die dem übergreifenden Zweck dienende Datenverarbeitung im Auftrag. Der Zuschnitt des Verfahrens ist von der verantwortlichen Stelle im Rahmen ihres Datenschutzkonzepts[671] zu bestimmen. Ob der Zuschnitt des Verfahrens einer risikoorientierten Betrachtung gerecht wird, ist für die Durchführung des Datenschutzaudits von entscheidender Bedeutung. Deshalb ist die sachliche Angemessenheit der Verfahrensbeschreibung von der verantwortlichen Stelle zu überprüfen, im Prüfergebnis zu beschreiben und zu begründen und vom betrieblichen oder behördlichen Datenschutzbeauftragten sowie vom Datenschutzgutachter zu kontrollieren und zu bestätigen.

Zu regeln sind die Voraussetzungen für verantwortliche Stellen, um erfolgreich am Datenschutzaudit teilnehmen zu können. Die Teilnahme ist freiwillig und kann jederzeit wieder aufgegeben werden.[672] Eine verantwortliche Stelle kann auch dann am Datenschutzaudit teilnehmen, wenn die Anwendung weiter reicht, als ihr Einflussbereich. Ihre Teilnahme soll nicht davon abhängen, dass andere, von ihr nicht beeinflussbare verantwortliche Stellen am Datenschutzaudit teilnehmen. In diesem Fall muss sie die Schnittstellen zu den anderen an der Anwendung beteiligten verantwortlichen Stellen überprüfen und transparent machen. Voraussetzung der Teilnahme am Datenschutzaudit ist die erfolgreiche Durchführung der oben genannten Schritte des Auditverfahrens.[673]

Einschränkungen für die Teilnahme verantwortlicher Stellen sind erforderlich, wenn ein Verfahren von mehreren verantwortlichen Stellen betrieben wird, die zueinander oder gemeinsam zu einem Dritten in einem Abhängigkeitsverhältnis stehen. In diesen Fällen könnte die Vergleichbarkeit der Ergebnisse gefährdet werden. Ein gemeinsam betriebenes Verfahren könnte in - aus Sicht des Datenschutzes und der Datensicherheit - „kritische“ und „unkritische“ Bestandteile zerlegt und zwischen einer „Mutter-“ und einer „Tochterorganisation“ oder zwischen mehreren „Tochterorganisationen“ der gleichen „Mutterorganisation“ aufgeteilt werden. Nehmen am Datenschutzaudit nur die verantwortlichen Stellen mit „unkritischen“ Bestandteilen der Verfahren teil, führt deren Auszeichnung durch ein Datenschutzauditzeichen zu Wettbewerbsverzerrungen bezogen auf den gesamten durch die „Mutterorganisation“ beherrschten Bereich. Daher können solche Stellen nur gemeinsam am Datenschutzaudit teilnehmen. Die Entscheidung für die Teilnahme liegt bei der „Mutterorganisation“. Sie kann die Teilnahme aller an dem Verfahren beteiligten „Tochterorganisationen“ durchsetzen.

Die Feststellung des Abhängigkeitsverhältnisses hängt von der jeweiligen Organisationsform der beteiligten verantwortlichen Stellen ab. Für Kapitalgesellschaften (Aktiengesellschaft, Gesellschaft mit beschränkter Haftung und Kommanditgesellschaft auf Aktien) beurteilt sich das Abhängigkeitsverhältnis nach § 17 AktG. Dies wird nach § 17 Abs. 2 AktG bei einer Mehrheitsbeteiligung vermutet. Im Fall einer GmbH & Co. KG sind die Grundsätze des § 17 AktG entsprechend anwendbar. Im Fall von Personengesellschaften liegt ein Abhängigkeitsverhältnis dann vor, wenn ein Gesellschafter in mehreren Gesellschaften die Teilnahme am Datenschutzaudit durchsetzen könnte. Verantwortliche Stellen des öffentlichen Rechts stehen in einem Abhängigkeitsverhältnis, sofern ein Weisungsrecht besteht. Eine die Teilnahme beeinflussende Abhängigkeit muss bei der Bestimmung und Prüfung der Anwendung untersucht und festgestellt werden.[674]

Die Teilnahme ausländischer Stellen wird sehr begrüßt. Sie darf allerdings nicht zu Wettbewerbsverzerrungen führen. Daher dürfen ausländische Stellen nur dann ein Datenschutzaudit-

671 S. Teil 3 Kap. 4.1.

672 S. näher *Roßnagel* 2000c, 84f.

673 S. näher *Roßnagel* 2000c, 74f., 78.

674 S. näher *Roßnagel* 2000c, 76 ff.

zeichen führen, wenn sie sich wie ihre deutschen Wettbewerber für ihr gesamtes Verfahren den Anforderungen an das Audit unterwerfen. Dadurch soll ausgeschlossen werden, dass innerhalb eines Verfahrens „kritische" Teilverfahren, die im Ausland betrieben werden, aus der Bewertung herausgenommen werden. Von ausländischen Teilnehmern kann nicht verlangt werden, dass sie in jeder Hinsicht die deutschen Vorschriften hinsichtlich Datenschutz und Datensicherheit erfüllen. Sie müssen sich aber in ihrer Datenschutzpolitik verpflichten und durch ihr Datenschutzmanagementsystem gewährleisten, dass in ihrem Verfahren materiell ein dem deutschen Datenschutzrecht vergleichbares Maß an Datenschutz und Datensicherheit sichergestellt ist. Die interne Datenschutzprüfung, die externe Überprüfung durch den Datenschutzgutachter und das Prüfergebnis müssen das gesamte von der verantwortlichen Stelle beherrschte Verfahren erfassen.[675]

Stellen, die personenbezogene Daten im Auftrag verarbeiten, sind keine verantwortlichen Stellen und betreiben kein Verfahren. Dennoch sollen sie am Datenschutzaudit teilnehmen können. Ihre Dienstleistungen sind Teil des Verfahrens auftraggebender Stellen und müssen von diesen in ihr Datenschutzaudit einbezogen werden. Die eigenständige Teilnahme der auftragnehmenden Stelle spart Aufwand und Kosten, da deren bestätigtes Prüfergebnis im Datenschutzaudit aller diese Dienstleistung nutzenden auftraggebenden Stellen verwendet werden kann. Für das Verfahren des Datenschutzaudits gelten die Vorschriften für verantwortliche Stellen sinngemäß. Die auftragnehmenden Stellen können eine oder mehrere Dienstleistungen auditieren und registrieren lassen. Da sie kein Verfahren verantwortlich betreiben und das Datenschutzaudit für ihre Dienstleistung nur einen Ausschnitt aus dem Verfahren betrifft, könnte die Verwendung des Datenschutzauditzeichens in der Öffentlichkeit zu Missverständnissen führen. Denn dieses zeigt an, dass der gesamte Prozess der Verarbeitung personenbezogener Daten eines Verfahrens unter einer risikoorientierten Sichtweise erfasst, verbessert und bewertet worden ist. Diese Beschränkung ist für die auftragnehmenden Stellen kein wesentlicher Nachteil. Sie können zum Nachweis ihrer Anstrengungen für Datenschutz und Datensicherheit das bestätigte Prüfergebnis verwenden. Für die auftraggebenden Stellen als ihre Kunden wird nicht das Datenschutzauditzeichen als solches, sondern das aussagekräftigere Prüfergebnis von entscheidender Bedeutung sein.

Die Vertrauenswürdigkeit des Datenschutzaudits hängt davon ab, dass ein externer, kompetenter, unabhängiger und objektiver Datenschutzgutachter die Einhaltung der Anforderungen prüft und bestätigt. Diese Prüfung sollte von privaten Gutachtern durchgeführt werden, deren Zuverlässigkeit, Unabhängigkeit und Fachkunde durch Zulassung und Kontrolle gewährleistet sein muss. Die Zulassung der Datenschutzgutachter könnte theoretisch von den Kontrollstellen übernommen werden. Dies setze aber zusätzliche Regelungen für die Anforderungen und das Verfahren voraus. Außerdem dürften die meisten Kontrollstellen für diese Aufgabe unzureichend ausgestattet sein. Bevor ihnen diese Aufgabe übertragen würde, müsste geprüft werden, ob sie hierzu bereit und in der Lage sind. Für die Zulassung der Gutachter bietet sich aber auch an, öffentlich bestellte und vereidigte Sachverständige nach § 36 GewO heranzuziehen. Ihre Zulassung wäre Aufgabe der Industrie- und Handelskammern. Diese Lösung erübrigt umfangreiche Regelungen zur Zulassung und Überwachung von Datenschutzgutachtern.[676] Bisher sind 105 Sachverständige für die elektronische Datenverarbeitung öffentlich bestellt. Allerdings müssen für das Sachgebiet des Datenschutzes und der Datensicherheit ein eigenes Anforderungsprofil und Kriterien für die Überprüfung der besonderen Sachkunde von Interessenten entwickelt werden. Dies sollte in Zusammenarbeit der

675 S. *Roßnagel* 2000c, 85

676 S. im Gegensatz hierzu die Regelungen zu den Umweltschutzgutachtern im Umweltauditgesetz vom 7.12.1995, BGBl. I, 1591, und in der Verordnung über das Verfahren zur Zulassung von Umweltgutachtern und Umweltgutachterorganisationen sowie zur Erteilung von Fachkenntnisbescheinigungen nach dem Umweltauditgesetz (UAG-Zulassungsverfahrensverordnung) vom 18.12.1995, BGBl. I, 1841.

Industrie- und Handelskammern mit den Kontrollstellen und dem Bundesamt für Sicherheit in der Informationstechnik erfolgen.[677]

Betriebliche oder behördliche Datenschutzbeauftragte haben Bedenken gegen das Datenschutzaudit vorgetragen, weil sie befürchteten, die Stellung des internen Datenschutzbeauftragten werden geschwächt, wenn das Ergebnis der internen Prüfung von einem externen Datenschutzgutachter bestätigt werden soll. Dies führe zu einer Konkurrenz mit den Aufsichtsaufgaben des Datenschutzbeauftragten und ermögliche sogar ein Audit entgegen der Auffassung der Datenschutzbeauftragten.[678] Diese Befürchtungen dürften unzutreffend sein, weil durch das Datenschutzaudit die Aufgaben des Datenschutzbeauftragten anwachsen und seine Bedeutung gestärkt werden.[679] Um die Befürchtungen auszuräumen und die Stellung des Datenschutzbeauftragten im Datenschutzaudit formell zu festigen, sollte das Audit von einem positiven Votum des Datenschutzbeauftragten und des externen Gutachters abhängig gemacht werden. Dadurch werden für das Audit sowohl der Sachverstand und die betriebsinternen Erfahrungen des Datenschutzbeauftragten der verantwortlichen Stelle als auch die betriebsübergreifenden Erfahrungen und die Unabhängigkeit des externen Gutachters genutzt.

Einer Regelung bedarf die Zuständigkeit und das Verfahren der Registrierung. Die Registrierung könnte einerseits – wie dies in Schleswig-Holstein praktiziert wird[680] – von der Kontrollstelle übernommen werden. Die meisten Kontrollstellen dürften aber für diese Aufgabe unzureichend ausgestattet sein. Bevor ihnen diese Aufgabe übertragen wird, müsste geprüft werden, ob sie hierzu bereit und in der Lage sind. Die andere Möglichkeit besteht darin, wie nach dem Umweltauditgesetz die zuständige Industrie- und Handelskammer mit der Registrierung zu betrauen. Auch für diese neue Aufgabe unterliegen die Industrie- und Handelskammern der Aufsicht der für sie zuständigen Aufsichtsbehörden. Aus fachlichen Gründen sollten Maßnahmen der Aufsicht über die Registrierungstätigkeit im Einvernehmen mit der zuständigen Kontrollstelle erfolgen. Da erst nach und nach die Teilnehmerzahlen zunehmen werden, sollte den Industrie- und Handelskammern ermöglicht werden, schriftlich zu vereinbaren, dass sie ihre Registrierungsaufgaben auf eine Industrie- und Handelskammer ganz oder teilweise übertragen. Dies kann auch länderübergreifend erfolgen.

Die Eintragung ins Datenschutzauditregister erfolgt auf Antrag der verantwortlichen Stelle. Sie wird vorgenommen, wenn sowohl der Datenschutzgutachter als auch der betriebliche oder behördliche Datenschutzbeauftragte bestätigen, dass die verantwortliche Stelle die materiellen Anforderungen erfüllt hat. Die Registrierungsstelle prüft, ob der Datenschutzgutachter die Prüfung in ausreichender Unabhängigkeit durchgeführt und seine Aufgaben ordnungsgemäß erfüllt hat. Sie gibt der zuständigen Kontrollstelle Gelegenheit zu Einwendungen.[681] Verfahren und Kosten können durch Satzung näher geregelt werden. Das Datenschutzaudit zielt nicht auf eine einmalige Feststellung der Konformität mit datenschutzrechtlichen Anforderungen und zusätzlicher Maßnahmen für Datenschutz und Datensicherheit, sondern auf eine ständige Einhaltung der Anforderungen und eine kontinuierliche Verbesserung von Datenschutz und Datensicherheit. Daher muss nach dem ersten Prüfzyklus das Datenschutzpro-

---

677 Soweit mit den Industrie- und Handelskammern der Erlass eigener Bestellvoraussetzungen für den Gutachter für Datenschutz und Datensicherheit im Einvernehmen mit den zuständigen Kontrollstellen und dem Bundesamt für Sicherheit in der Informationstechnik vereinbart werden kann, dürften sich eigene gesetzliche Regelungen erübrigen.

678 S. z.B. *Drews/Kranz*, DuD 1998, 98; *dies*., DuD 2000, 226; *Gola*, RDV 2000, 93; *Dieckmann/Eitschberger/Eul/Schwarzhaupt/Wohlrab*, DuD 2001, i.E.

679 S. hierzu *Roßnagel*, DuD 2000, 231.

680 S. Nr. 9 der Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH.

681 S. hierzu näher *Roßnagel* 2000c, 114 ff.

gramm fortgeschrieben werden und neben neuen Zielsetzungen und Maßnahmen auch – abhängig von den Maßnahmen und ihrer Dringlichkeit – einen neuen Zeitpunkt für die nächste Datenschutzprüfung vorsehen und im Prüfergebnis bekannt geben. Dieser darf nicht später als drei Jahre nach der letzten Prüfung liegen.[682]

Die Eintragung ins Datenschutzauditregister eröffnet die Möglichkeit, das Datenschutzauditzeichen und die Datenschutzerklärung für Werbezwecke zu nutzen. Die Verwendung des Zeichens muss jedoch mit dem Prüfgegenstand, dem Prüfumfang und der Prüftiefe übereinstimmen und darf keine Missverständnisse hervorrufen. Daher sind die Verwendungsmöglichkeiten des Zeichens zu begrenzen – auf Informationen über das auditierte Verfahren, auf allgemeine Image-Werbung der verantwortlichen Stelle[683] und auf Informationen über Datenschutz und Datensicherheit einzelner Tätigkeiten, Produkte und Dienstleistungen, die im Rahmen des auditierten Verfahrens genutzt werden.[684] Alle Informationen müssen dem Prüfergebnis entnommen sein und müssen auf dessen Bezugsmöglichkeit verweisen.[685] Dieser Hinweis kann auch aus einer elektronischen Verweisung auf das Prüfergebnis bestehen. Er soll Interessierten die Möglichkeit bieten, den Aussagegehalt des Zeichens bezogen auf das konkrete Verfahren nachzuvollziehen.

Die in den internationalen Normen für Managementsysteme durchgängig zu findenden Regelungen oder Anhänge mit Konkretisierungen für das Managementsystem und seine Prüfungen könnten entweder als Anhang zum Gesetz angefügt[686] oder als Empfehlung des zuständigen Ministeriums veröffentlicht werden.

Verantwortliche Stellen, die am Datenschutzaudit teilnehmen, sollten bevorzugt berücksichtigt werden, wenn es um Aufträge zur Verarbeitung personenbezogener Daten geht. Zumindest für öffentliche Stellen sollte diese Berücksichtigung zur Pflicht erhoben werden.[687] Als Erleichterungen für die Teilnehmer am Datenschutzaudit sollte vorgesehen werden, dass sie ihr Prüfergebnis an Stelle des Organisationsplans und des Datenschutz- und Datensicherheitskonzepts[688] verwenden können.

Das Datenschutzaudit setzt eine Regelung zum Datenschutzmanagement voraus, ist aber ansonsten nicht auf die übrigen in diesem Gutachten vorgeschlagenen Novellierungen angewiesen. Daher wird empfohlen, mit dem Datenschutzaudit und dem Datenschutzmanagement noch in dieser Legislaturperiode einen ersten Schritt der zweiten Stufe zur Novellierung des Datenschutzrechts zu realisieren.[689]

Die Regelung zum Datenschutzaudit könnte etwa in den folgenden vier Paragraphen erfolgen:

§ 1 Beteiligung am Datenschutzaudit

---

682 S. hierzu auch Nr. 9.2 und 10 der Anwendungsbestimmungen des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Behördenaudits nach § 43 Abs. 2 LDSG SH.

683 Etwa auf der Homepage, auf Hinweistafeln, auf Briefbögen, Broschüren, Presseinformationen und allgemeiner Werbung der verantwortlichen Stelle.

684 S. hierzu *Roßnagel* 2000c, 101 ff.

685 Das Prüfergebnis sollte sinnvoller Weise Teil der Datenschutzerklärung der verantwortliche Stelle sein - s. hierzu Teil 3 Kap. 2.3.

686 Diese sind im Gesetzentwurf von *Roßnagel* 1999 als Anhänge zum Datenschutzauditgesetz vorgesehen.

687 Eine ähnliche Regelung wurde im Entwurf für ein UGB in § 51 vorgeschlagen – s. zur Begründung UGB-KOM-E 1998, 547. Zur Zulässigkeit einer solchen Regelung nach europäischem und nationalem Vergabe- und Wettbewerbsrecht s. *Petri*, DuD 2001, 150.

688 S. zu beiden Teil 3 Kap. 4.1.

689 In diesem Fall müsste die Regelung zum Organisationsplan und zum Datenschutz- und Datensicherheitskonzept – s. Teil 3 Kap. 4.1 – ebenfalls geregelt und zumindest im folgenden § 1 in einer Nr. 2a vorgesehen werden, dass die verantwortliche Stelle ein Datenschutzmanagement einzurichten hat.

(1) Am Datenschutzaudit kann sich jede verantwortliche Stelle beteiligen, die den Datenschutz und die Datensicherheit eines oder mehrerer Verfahren fördern möchte. Ein Verfahren ist der einer übergreifenden Zielsetzung einer oder mehrerer verantwortlicher Stellen dienende Prozess des systematischen Zusammenwirkens technisch-organisatorischer Komponenten, in dem personenbezogene Daten verarbeitet werden.

(2) Zur Eintragung in das Datenschutzauditregister muss eine verantwortliche Stelle auf der Grundlage eines Datenschutz- und Datensicherheitskonzepts

1. *eine Datenschutzpolitik mit Gesamtzielen und Handlungsgrundsätzen festlegen, in der sie sich verpflichtet, alle einschlägigen Datenschutzvorschriften einzuhalten und Datenschutz und Datensicherheit unter wirtschaftlich vertretbarem Einsatz der besten verfügbaren Technik kontinuierlich zu verbessern oder auf höchstem Stand zu erhalten,*
2. *ein Datenschutzprogramm erstellen, das konkrete Maßnahmen und Fristen zur Umsetzung der Datenschutzpolitik festlegt,*
3. *eine Datenschutzprüfung durchführen, die feststellt, ob das Datenschutzmanagementsystem die Umsetzung der Datenschutzpolitik und des Datenschutzprogramms sicherstellt,*
4. *anhand eines schriftlichen Prüfergebnisses vom Datenschutzbeauftragten sowie von einem nach § 36 der Gewerbeordnung zugelassenen Datenschutzgutachter bestätigen lassen, dass die Anforderungen an ein Datenschutzaudit eingehalten werden,*
5. *das bestätigte Prüfergebnis der zuständigen Registrierungsstelle übermitteln und frei zugänglich machen.*

(3) Wird ein Verfahren von mehreren verantwortlichen Stellen betrieben, die zueinander oder gemeinsam zu einem Dritten in einem Abhängigkeitsverhältnis stehen, können sie nur gemeinsam am Datenschutzaudit teilnehmen.

(4) Ausländische verantwortliche Stellen können sich am Datenschutzaudit beteiligen, wenn sie ihre Verfahren den Anforderungen dieses Gesetzes unterwerfen und hinsichtlich der Einhaltung der für sie einschlägigen Datenschutzvorschriften ein dem deutschen Datenschutzrecht vergleichbares Maß an Datenschutz und Datensicherheit gewährleisten.

(5) Stellen, die personenbezogene Daten im Auftrag verarbeiten und den Datenschutz und die Datensicherheit einer oder mehrerer Auftragsdienstleistungen verbessern wollen, können sich am Datenschutzaudit beteiligen. Für sie gelten die Vorschriften dieses Unterabschnitts mit Ausnahme von § 4 entsprechend. Bestätigte Prüfergebnisse können in Datenschutzaudits auftraggebender Stellen Verwendung finden.

§ 2 Registrierung

(1) Die Registrierung auditierter Verfahren wird den Industrie- und Handelskammern als zuständiger Registrierungsstelle übertragen. Aufsichtsmaßnahmen werden von der Aufsichtsbehörde im Einvernehmen mit der zuständigen Kontrollstelle getroffen.

(2) Die Industrie- und Handelskammern übermitteln am Ende eines jeden Jahres ein fortgeschriebenes Verzeichnis der registrierten Verfahren an den Bundesbeauftragten für den Datenschutz. Das Verzeichnis wird der Öffentlichkeit zugänglich gemacht.

(3) Die Industrie- und Handelskammern können schriftlich vereinbaren, dass die von ihnen nach Absatz 1 Satz 1 wahrgenommenen Aufgaben auf eine Industrie- und Handelskammer des gleichen oder eines anderen Landes ganz oder teilweise übertragen werden. Die Vereinbarung bedarf der Genehmigung der Aufsichtsbehörde im Einvernehmen mit der zuständigen Kontrollstelle.

(4) Die Industrie- und Handelskammern können das Verfahren für die Registrierung durch Satzung näher regeln. Die Satzung bedarf der Genehmigung entsprechend Absatz 3 Satz 2. Die Satzungen gelten auch für verantwortliche Stellen, die nicht Mitglied der Kammer sind.

(5) Einheitliche Grundsätze für das Verfahren der Registrierung können mit Zustimmung des Bundesrats durch Rechtsverordnung des für den Datenschutz zuständigen Bundesministers festgelegt werden.

(6) Für die Eintragung, die Aussetzung und die Streichung der Eintragung sowie die Prüfung der Beibehaltung der Eintragung werden Kosten (Gebühren und Auslagen) erhoben. Die Industrie- und Handelskammern werden ermächtigt, die Höhe der Kosten durch Satzung zu bestimmen. Absatz 4 Satz 2 und 3 gilt entsprechend.

§ 3 Eintragung ins Register

(1) Das Verfahren der verantwortlichen Stelle wird in das Register eingetragen, wenn

1. *das Prüfergebnis vom betrieblichen oder behördlichen Datenschutzbeauftragten und von einem unabhängigen Datenschutzgutachter bestätigt worden ist,*
2. *keine Tatsachen die Annahme rechtfertigen, dass der Datenschutzgutachter gegen seine Pflichten aus diesem Gesetz verstoßen hat,*
3. *keine Tatsachen die Annahme rechtfertigen, dass die verantwortliche Stelle eine Anforderung dieses Gesetzes nicht erfüllt,*
4. *die verantwortliche Stelle die für die Registrierung zu entrichtenden Kosten bezahlt hat.*

Für Satz 1 Nr. 1 gilt § 319 Abs. 2 und 3 des Handelsgesetzbuches entsprechend.

(2) Vor der Eintragung eines Verfahrens gibt die Registrierungsstelle der zuständigen Kontrollstelle Gelegenheit, sich innerhalb einer Frist von einem Monat zu der beabsichtigten Eintragung zu äußern. Teilt die Kontrollstelle einen Verstoß gegen die rechtlichen Anforderungen an Datenschutz und Datensicherheit mit, den die verantwortliche Stelle bestreitet, so ist die Entscheidung über die Eintragung bis zur Klärung zwischen der für den Datenschutz zuständigen Behörde und der verantwortlichen Stelle auszusetzen.

(3) Zur Beibehaltung der Eintragung müssen verantwortliche Stellen entsprechend ihrem Datenschutzprogramm, spätestens jedoch alle drei Jahre, eine Datenschutzprüfung durchführen und eine Fortführung der Eintragung nach den Voraussetzungen des Absatzes 1 beantragen.

(4) Die Eintragung wird gestrichen, wenn die verantwortliche Stelle trotz Anhörung die Anforderungen des Gesetzes nicht erfüllt.

§ 4 Datenschutzauditzeichen

(1) Verantwortliche Stellen, die als Teilnehmer am Datenschutzaudit registriert sind, dürfen das in Anhang I beschriebene Datenschutzauditzeichen für Informationen über das auditierte Verfahren und allgemeine Informationen über die verantwortliche Stelle verwenden. Sie haben dabei auf die Teilnahme am Datenschutzaudit für das jeweilige Verfahren und die Bezugsmöglichkeit des Prüfergebnisses, die Registrierungsnummer sowie auf die Befristung des Audits hinzuweisen.

(2) Verantwortliche Stellen können das Zeichen ferner in Verbindung mit Informationen über Datenschutz und Datensicherheit bei Tätigkeiten, Produkten und Dienstleistungen im Rahmen des Verfahrens verwenden. Die Informationen müssen sich auf Datenschutz und Datensicherheit in dem auditierten Verfahren beziehen und dem Prüfergebnis entnommen sein. Sie dürfen nicht missverständlich und irreführend und müssen nachprüfbar und relevant sein.

(3) Das Zeichen darf nicht auf Produkten oder ihrer Verpackung, auf Vergleichen zwischen Produkten, Tätigkeiten und Dienstleistungen sowie unbeschadet der Absätze 1 und 2 auf Werbung für Produkte, Tätigkeiten und Dienstleistungen angebracht werden.

4.3 Förderung datenschutzgerechter Technik

Da das Datenschutzrecht auf eine „Allianz" mit Datenschutztechnik angewiesen ist, um seine Ziele erfüllen zu können,[690] muss es datenschutzgerechte Technik fordern und fördern. Zu diesem Zweck sollten zumindest drei Regelungen vorgesehen werden. Die Hersteller sollten verpflichtet werden, für die Gestaltung ihrer Produkte zumindest die Erfüllung einiger zentraler Produktanforderungen zu überprüfen. Wer datenschutzgerechte Produkte herstellt, sollte die Möglichkeit erhalten, diese zertifizieren zu lassen und mit dem Zertifikat werben zu können. Schließlich sollten die verantwortlichen Stellen aufgefordert werden, datenschutzgerechte Produkte zu verwenden.

4.3.1 Anforderungen an Entwicklung und Herstellung

Maßnahmen zum Schutz der informationellen Selbstbestimmung können von den verantwortlichen Stellen oft deshalb nicht ergriffen werden, weil die verwendeten Produkte der Informations- und Kommunikationstechnik diese Maßnahmen nicht zulassen. Um sicherzustellen, dass die Anforderungen, die an die verantwortliche Stelle zur Gewährleistung von Datenschutz und Datensicherheit gestellt werden,[691] auch erfüllt werden können, müssen Anforderungen an Datenschutz und Datensicherheit auch schon in der Entwicklung und Herstellung der Produkte erfüllt werden. Zu diesem Zweck sollten im Gesetz materielle Anforderungen formuliert werden. Sie zu erfüllen entspricht der öffentlich-rechtlichen Produktverantwortung der Hersteller und Vertreiber.[692] Aufgrund der Vielfalt und Multifunktionalität der Produkte, der Globalität ihres Marktes, möglicher Zielkonflikte in der Konkretisierung der Anforderungen sowie der Vollzugsschwierigkeiten sollten keine Erfüllungspflichten, sondern Prüfpflichten formuliert werden.[693] Diese können für einzelne Bereiche mit Zielfestlegungen der Bundesregierung verbunden werden.[694]

Eine solche Vorschrift könnte etwa folgende Regelungen enthalten:

(1) Hersteller haben bei Entwicklung und Herstellung von Produkten der Informationstechnik (Hardware, Software und automatisierte Verfahren) zu prüfen, ob und wie es möglich ist,

1. die Verarbeitung personenbezogener Daten zu vermeiden oder zu vermindern,

2. die Transparenz über die Funktionen und die Verarbeitung personenbezogener Daten für den Nutzer herzustellen oder zu erhöhen,

3. werkseitig die für den Nutzer datenschutzfördernde und sichere Voreinstellung zu wählen,

4. die Möglichkeiten des Nutzers zur Kontrolle über die Verarbeitung personenbezogener Daten und Sicherheitseigenschaften zu schaffen oder zu verbessern,

5. die Verwendung von Funktionen und personenbezogenen Daten für nicht vorgesehene Zwecke zu verhindern oder zumindest zu erschweren,

---

690 S. zu dieser Forderung z.B. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 259 ff.; *Roßnagel* 1993, 241 ff.; *ders.* 2001, 13 ff.; *Simitis* 1996, 35 ff.; *Bizer* 1999, 28 ff.; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 ff. Aus technischer Sicht *Pfitzmann*, DuD 1999, 405 ff.

691 S. z.B. Teil 3 Kap. 5.6.

692 S. z.B. für den insoweit vergleichbaren Bereich des Umweltrechts z.B. § 22 ff. KrW-/AbfG; *Beckmann*, UPR 1996, 41 ff.; UGB-KOM-E 1998, 671, 679.

693 Vorbild könnte insoweit § 118 im Entwurf eines UGB sein – s. UGB-KOM-E 1998, 679f., 682.

694 S. hierzu näher Teil 3 Kap. 6.2.

6. personenbezogene Daten für unterschiedliche Zwecke getrennt zu verarbeiten,

7. die sichere und datenschutzgerechte oder datenschutzfördernde Verwendung der Produkte zu kontrollieren.

Die Ergebnisse der Prüfung sind bei der Entwicklung und Herstellung von Produkten der Informationstechnik zu berücksichtigen.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die Produkte der Informationstechnik zu bestimmen, bei deren Entwicklung und Herstellung die Prüfung nach Absatz 1 zu dokumentieren ist.

(3) Hersteller und Vertreiber von Produkten der Informationstechnik weisen in geeigneter Weise auf Risiken und förderliche Eigenschaften für Datenschutz und Datensicherheit hin und geben Empfehlungen zu ihrer datenschutzgerechten oder datenschutzfördernden und sicheren Verwendung.

Die genannten Kriterien der Produktentwicklung und -gestaltung[695] sind ausreichend flexibel, um in unterschiedlichen Anwendungsfeldern der Informationstechnik Verwendung finden zu können, zugleich aber auch ausreichend konkret, um aus ihnen technische Gestaltungsziele und -vorschläge ableiten und Gestaltungsalternativen bewerten zu können.[696]

Die Ergebnisse der Prüfung sind bei der Entwicklung und Herstellung von Produkten der Informations- und Kommunikationstechnik zu berücksichtigen. Unterlässt der Hersteller die Prüfung und die Berücksichtigung der Ergebnisse, kann dies unter Umständen eine Sorgfaltspflichtverletzung darstellen. Von daher liegt es im Selbstinteresse des Herstellers, die Prüfung und ihre Berücksichtigung zu dokumentieren. Um nicht flächendeckend alle Hersteller von Produkten der Informations- und Kommunikationstechnik mit Dokumentationsaufwand zu belasten, sollte Durchführung, Form und Inhalt einer solchen Dokumentation ihnen überlassen werden.

In bestimmten Bereichen (etwa im Gesundheitsbereich) oder für bestimmte Produkte (z.B. Personaldatenverarbeitungssysteme), von denen typischerweise relevante Risiken für Datenschutz und Datensicherheit ausgehen, kann es jedoch angebracht sein, bestimmte Dokumentationspflichten vorzusehen. Aus diesem Grund sollte die Bundesregierung ermächtigt werden, durch Rechtsverordnung die Produkte der Informations- und Kommunikationstechnik zu bestimmen, bei deren Entwicklung und Herstellung die Prüfung nach Absatz 1 zu dokumentieren ist.

Auch wenn die Produkte der Informations- und Kommunikationstechnik datenschutzgerecht oder datenschutzfördernd gestaltet sind, hilft dies für die Praxis des Datenschutzes wenig, wenn die Nutzer diese Datenschutz fördernden Eigenschaften nicht zu nutzen wissen. Umgekehrt könnten Datenschutz und Datensicherheit in der Praxis deutlich verbessert werden, wenn die Nutzer wüssten, auf welche Risiken sie achten sollten und wie sie diese vermeiden könnten. Sie darüber aufzuklären, ist in erster Linie eine Aufgabe des Staats, die in seine Infrastrukturverantwortung fällt.[697] Aber auch diejenigen, die Produkte der Informations- und Kommunikationstechnik herstellen oder vertreiben, müssen einen Teil dieser Aufgabe übernehmen. Von ihnen sollte zumindest gefordert werden, dass sie in geeigneter Weise auf Risi-

---

695 S. zu ihrer Ableitung aus verfassungsrechtlichen Vorgaben z.B. *Roßnagel* 1993, 278 ff.; *Hammer/Pordesch/Roßnagel* 1993, 43 ff.; *Roßnagel/Pordesch*, DuD 1994, 82 ff.

696 S. zur Konkretisierung solcher Kriterien z.B. die Methode „*K*onkretisierung *r*echtlicher *A*nforderungen (KORA)" – *Pordesch/Hammer/Roßnagel* 1991; *Hammer/Pordesch/Roßnagel* 1993; *Hammer/Pordesch/Roßnagel/Schneider* 1994; *Roßnagel/Pordesch*, DuD 1994, 82 ff.; *Roßnagel/Schroeder* 1999; *Idecke-Lux* 2000; s. auch zur Fortentwicklung der Methode KORA *Hammer* 1999; s. auch *Bizer* 1999, 54 ff.

697 S. hierzu Teil 3 Kap. 5.2.

ken und förderliche Eigenschaften ihrer Produkte hinweisen und Empfehlungen zu einer datenschutzgerechten und sicheren Verwendung ihrer Produkte geben.

Hersteller und Vertreiber könnten ihrer Aufklärungspflicht auch dadurch nachkommen, dass sie Gutscheine für eine Beratung ausgeben, die die Käufer kostenlos bei geeigneten Beratungsstellen einlösen. Dadurch könnte – besser als durch einen schriftlichen Hinweis – die Aufklärung über Datenschutz und Datensicherheit den Vorkenntnissen und Interessen des Käufers gemäß interaktiv erfolgen. Da das erforderliche Netz von Beratungsstellen noch nicht aufgebaut ist, kann eine entsprechende rechtliche Regelung derzeit noch nicht empfohlen werden. Ein solches Netz aufzubauen, könnte aber Gegenstand einer Zielfestlegung der Bundesregierung sein,[698] wobei eine Verbindung mit anderen Aufklärungszwecken – wie zum Beispiel Verbraucherschutz – zu wünschenswerten Synergieeffekten führen würde.

4.3.2 Produktzertifizierung

Zur Erleichterung der Auswahl von datenschutzgerechten Produkten der Informations- und Kommunikationstechnik sollte eine gesetzlich geregelte Produktzertifizierung angeboten werden. Während das Datenschutzaudit Datenschutzkonzepte, die von einem Datenschutzmanagement umzusetzen sind, in einem Systemaudit evaluiert, ist für Hard- und Software sowie automatisierte Verfahren ein Produktaudit in Form einer Zertifizierung erforderlich. Bei dieser geht es nicht um die wiederholte Überprüfung und Bewertung von Anstrengungen zur Verbesserung des Datenschutzes, sondern um die einmalige Bewertung der Datenschutz- und Datensicherheitseigenschaften einer bestimmten Version eines Produkts. Eine solche Produktzertifizierung ist in Schleswig-Holstein nach § 4 Abs. 2 LDSG vorgesehen und seit April 2001 in einer Gütesiegelverordnung umgesetzt.[699]

Die Datenschutzzertifizierung erfolgt auf Antrag des Herstellers oder Anbieters. Es macht wenig Sinn, wenn die vielen tausend Anwender eines Datenverarbeitungssystems oder -programms dieses viel tausendfach zertifizieren lassen.[700] Vielmehr sollte allein der jeweilige Hersteller oder Anbieter für das System oder Programm eine einzige Zertifizierung erhalten, auf die sich dann alle Anwender verlassen können. Die verantwortlichen Stellen sollten – soweit vorhanden – zertifizierte Datenverarbeitungssysteme und -programme in ihrer Datenverarbeitung einsetzen. Verwenden sie zertifizierte Produkte, soll eine Vermutung bestehen, dass mit ihrer richtigen Verwendung die jeweils relevanten Anforderungen des Datenschutzes erfüllt sind.

Anforderungen an die Produkte ergeben sich zum Einen aus den Kriterien, die von den Herstellern bei der Prüfung für die Entwicklung und Herstellung zu beachten sind.[701] Diese sollten in Empfehlungen des Bundeswirtschaftsministeriums weiter konkretisiert werden. Sie sind zum Anderen anwendungsspezifisch vom Hersteller zusammen mit dem Prüfer etwa in Form von „Protection Profiles“ entsprechend den „Common Criteria“ zu präzisieren. Soweit dies möglich ist, sollten Vertreter der Anwender und Nutzer an der Erstellung der „Profiles“ beteiligt werden. Zumindest sollte ihnen Gelegenheit hierzu gegeben werden. Wird das Zertifikat zur Werbung für das Produkt verwendet, ist auf das „Profile“ hinzuweisen. Es ist der Öffentlichkeit zugänglich zu machen, insbesondere dadurch, dass ein einfacher Zugriff im Rahmen elektronischer Medien ermöglicht wird.

---

698 S. hierzu Teil 3 Kap. 6.2.

699 S. Landesverordnung über ein Datenschutzaudit vom 3.4.2001, GS Sch.-H. II, Gl. Nr. 204-4-4-2 – s. näher *Bäumler*, DuD 2001, 252.

700 In der Regel verfügen die Anwender auch nicht über die für eine Zertifizierung des Produkts notwendige Detailinformation, wie über Quelltexte und verwendete Hilfsmittel, Entwurfsdokumentation und ähnliches.

701 S. hierzu Teil 3 Kap. 4.3.1.

Die Prüfung der Produkte sollte – wie beim Datenschutzaudit – von privaten Gutachtern durchgeführt werden, deren Zuverlässigkeit, Unabhängigkeit und Fachkunde durch Zulassung und Kontrolle gewährleistet sein muss. Die Zulassung der Gutachter könnte ebenfalls den Industrie- und Handelskammern im Rahmen des § 36 GewO übertragen werden.[702]

Das Siegel sollte nicht vom Gutachter, sondern von einer dritten Stelle vergeben werden, die die Korrektheit des Gutachtens und der Arbeit des Gutachters überprüft. Hierfür kämen einerseits – wie dies in Schleswig-Holstein praktiziert wird[703] – die Kontrollstellen in Frage. Die meisten Kontrollstellen dürften aber für diese Aufgabe unzureichend ausgestattet sein. Bevor ihnen diese Aufgabe übertragen wird, müsste geprüft werden, ob sie hierzu bereit und in der Lage sind. Die andere Möglichkeit besteht darin, wie beim Datenschutzaudit die für den Antragsteller zuständige Industrie- und Handelskammer mit der Vergabe des Siegels zu betrauen. Sie sollte – ebenso wie beim Audit – die Möglichkeit haben, diese Aufgabe auf eine andere Industrie- und Handelskammer zu übertragen sowie das Verfahren und die Kosten für die Vergabe des Siegels durch Satzung näher zu regeln. Wird das Siegel von der Industrie- und Handelskammer erteilt, hat sie der zuständigen Kontrollstelle Gelegenheit zu Einwendungen zu geben.

(1) Produkten der Informationstechnik kann auf Antrag des Herstellers oder Vertreibers ein Siegel für Datenschutz und Datensicherheit nach Anlage II erteilt werden, wenn für diese die vorbildliche Einhaltung der Anforderungen an Entwicklung und Herstellung (§ X[704]) nachgewiesen worden ist. Das Siegel für Datenschutz und Datensicherheit ist unter Angabe der besonderen Eigenschaften für Datenschutz und Datensicherheit für eine bestimmte Zeit, die zwei Jahre nicht überschreiten darf, zu erteilen.

(2) Das Siegel für Datenschutz und Datensicherheit darf in der Werbung für dieses Produkt unter Angabe der besonderen Eigenschaften für Datenschutz und Datensicherheit verwendet werden. Das Gütezeichen muss die Registrierungsnummer und die Befristung der Gültigkeit enthalten. Auf eine genaue Beschreibung der besonderen Eigenschaften ist hinzuweisen. Sie ist der Öffentlichkeit kostenlos zugänglich zu machen.

(3) Das Siegel wird von der für den Antragsteller zuständigen Industrie- und Handelskammer auf der Grundlage des Gutachtens eines nach § 36 der Gewerbeordnung bestellten und vereidigten Sachverständigen für Datenschutz und Datensicherheit erteilt. § 2 Abs. 1 Satz 2 sowie Abs. 2 bis 6 gilt entsprechend. Der zuständigen Kontrollstelle ist entsprechend § 3 Abs. 2 Gelegenheit zu Einwendungen zu geben.[705]

(4) Die Erteilung des Siegels für Datenschutz und Datensicherheit kann jederzeit widerrufen werden, wenn sich nachträglich herausstellt, dass eine nach Absatz 1 zu benennende Eigenschaft nicht vorlag oder entfallen ist.

Anzustreben ist künftig eine Produktzertifizierung, die nicht erst nach dem Markteintritt eines Produkts beginnt, sondern bereits entwicklungsbegleitend erfolgt. Schon die Entwicklungsabteilungen der Hersteller wären so gehalten, datenschutzfördernde Techniken in die Produktgestaltung aufzunehmen. Nachträgliche Verbesserungen der Produkte aus Sicht des Datenschutzes entfielen. Darüber hinaus könnten Hersteller von Beginn an mit dem Zertifikat werben. Eine entsprechende Privilegierung zertifizierter Produkte bei öffentlichen Ausschrei-

---

[702] S. hierzu näher Teil 3 Kap. 4.2.

[703] *Bäumler*, DuD 2001, 252.

[704] S. den Regelungsvorschlag in Teil 3 Kap. 4.3.1.

[705] Die Verweisungen beziehen sich auf den Regelungsvorschlag zum Datenschutzaudit in Teil 3 Kap. 4.2.

bungen böte einen zusätzlichen Anreiz für die Hersteller, datenschutzfördernde Technik zu entwickeln.[706]

4.3.3 Absatzförderung

Da das Datenschutzrecht auf die Verbreitung datenschutzgerechter Produkte angewiesen ist, muss es auch deren Absatz fördern. Daher sollte für verantwortliche Stellen des öffentlichen Bereichs die Verpflichtung vorgesehen werden, bei der Gestaltung von Prozessen zur Verarbeitung personenbezogener Daten vorrangig datenschutzfördernde Produkte zu verwenden. Diese können leicht daran erkannt werden, dass sie zertifiziert sind. Nach dieser Verpflichtung soll die öffentliche Hand in doppelter Funktion tätig werden, nämlich in Vorbild- und in Marktfunktion. Die Vorbildfunktion des Staats ist in der Weise angesprochen, dass er mit gutem Beispiel vorangehen sollte, wenn es darum geht, Belange des Datenschutzes bei der Beschaffung zu berücksichtigen. Die Verwendung datenschutzgerechter oder datenschutzfördernder Produkte durch staatliche Stellen kann bei Bürgern und Unternehmen einen Nachahmungseffekt bewirken, wenn sie sehen, dass es möglich und umsetzbar ist, datenschutzgerechte Produkte zu verwenden. Die gezielte Nachfrage durch die öffentliche Hand kann darüber hinaus den Bekanntheitsgrad und den Marktanteil datenschutzgerechter Produkte fördern und damit ihre Markteinführung und Diffusion ermöglichen oder beschleunigen.

Diese Verpflichtung kann sich am Beispiel des § 37 KrW-/AbfG sowie an vergleichbaren Vorschriften der Landesabfallgesetze[707] orientieren. Während § 37 KrW-/AbfG jedoch nur eine Prüfpflicht vorsieht,[708] enthalten die Landesabfallgesetze Verwendungspflichten. Auch der Entwurf für ein UGB schlug in § 51 eine Verpflichtung zur Verwendung umweltgerechter Produkte vor.[709] Aus Gründen des Haushaltsrecht sollte die Verpflichtung allerdings davon abhängig gemacht werden, dass Produkte für den vorgesehenen Verwendungszweck geeignet sind und dadurch keine unzumutbaren Mehrkosten entstehen.

Eine Regelung könnte etwa folgendermaßen lauten:

Öffentliche Stellen haben bei der Gestaltung von Prozessen zur Verarbeitung personenbezogener Daten vorrangig Produkte zu verwenden, die den Anforderungen an Entwicklung und Herstellung (§ X[710]) entsprechen, sofern diese Produkte für den vorgesehenen Verwendungszweck geeignet sind und dadurch keine unzumutbaren Mehrkosten entstehen. Bei der Vergabe von Aufträgen zur Datenverarbeitung sollen öffentliche verantwortliche Stellen berücksichtigen, ob der Auftragnehmer am Datenschutzaudit teilnimmt.

Die Beschaffungsverpflichtung kann in einem Bundesgesetz nur für Stellen vorgesehen werden, die der Bundesverwaltung zuzurechnen sind. Für Landesbehörden ist zu beachten, dass gemäß Art. 84 Abs.1 und Art. 85 Abs. 1 GG dem jeweiligen Land deren Einrichtung als Teil seiner Organisationsgewalt obliegt. Hierbei erstreckt sich die „Einrichtung" der Behörden auch auf deren Ausstattung mit Sachmitteln.[711] Da der Anwendungsbereich des Gesetzes die verantwortlichen Stellen der Länder ohnehin ausnimmt, entsteht insoweit kein Konflikt. Auch eine spezifische Ausnahmeregelung erscheint nicht erforderlich.

---

706 S. das folgende Kapitel.

707 S. z.B. § 5 LAbfG BW; Art. 8 Abs. 2 Nr. 1 BayAbfG; § 3 Abs. 1 HambAbfG; § 3 NAbfG; § 2 Abs. 1 AbfARG M-V; § 2 Abs. 2 AbfWAG Rh.-Pf.; § 1 Abs. 3 EGAB-Sachs.

708 Der Bundesrat hatte eine Verpflichtung vorgeschlagen, s. BR-Drs. 528/90 (Beschluss) und BT-Drs. 12/631, Einleitung Rn. 92.

709 S. zur Begründung UGB-KOM-E 1989, 547. Zur Zulässigkeit einer solchen Regelung nach europäischem und nationalem Vergabe- und Wettbewerbsrecht s. *Petri*, DuD 2001, 150.

710 S. den Regelungsvorschlag in Teil 3 Kap. 4.1.

711 S. hierzu auch UGB-KOM-E 1989, 545.

Für verantwortliche Stellen des nicht öffentlichen Bereichs sollte zur Wahrung der verfassungsrechtlich gewährleisteten wirtschaftlichen Entscheidungsautonomie lediglich eine Prüfpflicht vorgesehen werden, datenschutzgerechte Produkte zu verwenden. Diese Prüfung wird im Rahmen des Datenschutzmanagementsystems durchgeführt und ihr Ergebnis im Datenschutzkonzept dokumentiert.[712] Nehmen verantwortliche Stellen am Datenschutzaudit teil, werden sie ohnehin in dem ihnen möglichen Umfang datenschutzgerechte Produkte verwenden.[713]

5. Selbstdatenschutz

Da Staat und Recht in globalen Netzen und einer Welt allgegenwärtiger Datenverarbeitung nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Bürger zu schützen, ist es erforderlich, dass nach Ausschöpfen aller bereits genannten Möglichkeiten zum Schutz der Selbstbestimmung dem Bürger ermöglicht wird, Mittel zu ergreifen, um seine informationelle Selbstbestimmung selbst zu schützen.[714]

Selbstdatenschutz darf nicht isoliert gesehen werden. Es genügt nicht, sich darauf zu beschränken, den betroffenen Personen ein Maßnahmenbündel anzubieten und es ihnen im Übrigen zu überlassen, die zu ihrem Schutz notwendigen Vorkehrungen zu treffen.[715] Soweit jedoch die Möglichkeiten der normativen Verhaltenssteuerung und des Systemdatenschutzes ausgeschöpft sind, kann auf die Möglichkeiten des Selbstdatenschutzes als ergänzende Maßnahmen nicht verzichtet werden.[716]

5.1 Recht auf Anonymität und Pseudonymität

Das wohl wichtigste Mittel des Selbstdatenschutzes ist die Möglichkeit, anonym oder pseudonym zu handeln. In der Offline-Welt ist diese Möglichkeit selbstverständlich. Jeder kann beim Bäcker anonym seine Brötchen kaufen oder sich unter Pseudonym bei einer Behörde erkundigen. Im Internet und in der künftigen Welt allgegenwärtiger Datenverarbeitung besteht diese Selbstverständlichkeit nicht mehr, weil jede Handlung mit technischer Notwendigkeit Datenspuren hinterlässt. Diese Möglichkeit muss erst künstlich hergestellt werden, indem Verfahren für anonymes und pseudonymes Handeln geschaffen werden.

Im gleichen Maß, wie die Möglichkeit, ohne Datenspuren zu handeln, entschwindet, steigt ihre Bedeutung. Da personenbezogene Daten, die im Rahmen vernetzter Informationsverarbeitung entstanden sind und verarbeitet werden,[717] für die betroffene Person faktisch nicht mehr kontrollierbar sind und ihre Löschung praktisch nicht mehr durchgesetzt werden kann,[718] kommt es entscheidend auf die vorbeugende Vermeidung personenbezogener Daten an.[719]

---

712 S. Teil 3 Kap. 4.1.

713 S. Teil 3 Kap. 4.2.

714 S. *Roßnagel*, ZRP 1997, 26 ff.

715 *Simitis*, DuD 2000, 725.

716 s. Teil 2 Kap. 2.2.

717 Bei einem schlichten Internetkauf führt die Kauf- und Bezahltransaktion nicht nur zu einem Datenfluss zum Händler, sondern zur Datenübermittlung an eine Vielzahl von weit verstreuten Stellen, auch wenn der betroffenen Person nur der Händler selbst sichtbar ist.

718 Angesichts unbegrenzt großer Speicherkapazitäten und der Proliferation von Daten in offenen Netzen bleibt jedes digitale Datum immer irgendwo potenziell verfügbar. Normative Regelungen zur rechtzeitigen Löschung personenbezogener Daten stoßen hier an ihre Wirksamkeitsgrenzen. – s. auch *Roßnagel/Bizer* 1995, 46 für das parallele Problem bei Medienarchiven.

719 S. Teil 1 Kap.1.1, Teil 2 Kap. 1.3 und 2.2 und Teil 3 Kap. 3.4.2 und 3.4.3; zur Datenvermeidung durch Anomymität und Pseudonymität s. *Roßnagel/Scholz*, MMR 2000, 721.

Bereits unter dem Stichwort der Erforderlichkeit wurde dargelegt, dass die verantwortlichen Stellen verpflichtet sein sollten, soweit im Rahmen der Datenverarbeitung eine Identifizierung nicht erforderlich ist, auf einen Personenbezug der Daten zu verzichten und, soweit dies im Rahmen der Technik- und Verfahrensgestaltung möglich ist, anonymes oder pseudonymes Handeln anzubieten oder zumindest zu akzeptieren.[720]

Diese Verpflichtung auf Seiten der verantwortlichen Stelle sollte um ein korrespondierendes Recht auf Anonymität und Pseudonymität auf Seiten der betroffenen Person ergänzt werden.[721] Dieses soll als Ausdruck der informationellen Selbstbestimmung der betroffenen Person ein Identitätsmanagement ermöglichen. Sie soll das Recht haben, grundsätzlich unter der von ihr gewünschten Identität zu handeln.[722]

Ein solches Recht ist allerdings durch die Rechte Dritter und durch Allgemeininteressen beschränkt und wird daher nur in seltenen Fällen einklagbar sein. Es rechtfertigt nicht einen Eingriff in die Vertragsfreiheit der verantwortlichen Stelle und zwingt diese daher nicht zum Abschluss von Verträgen mit anonym oder pseudonym Handelnden. Auch befreit es nicht von Identifizierungspflichten, die aus Gemeinwohlgründen gesetzlich festgelegt sind.

Ein solches Recht bringt aber eine wichtige Grundregel für den Persönlichkeitsschutz und die informationelle Selbstbestimmung in der Informationsgesellschaft zum Ausdruck.[723] Es lässt Anonymität und Pseudonymität nicht als exotische Ausnahme, sondern als Ausdruck der Handlungsfreiheit und damit als normativen Regelfall erscheinen. Dadurch verändert es Erwartungshaltungen und Begründungslasten. Im Privatrecht wird es seine rechtliche Wirkung vor allem dadurch entfalten, dass es die Auslegung von unbestimmten Rechtsbegriffen beeinflusst. Im Kontakt mit der Verwaltung zwingt es dazu, im Einzelfall zu prüfen, ob es vertretbar ist, auf die Verpflichtung zur aktuellen Identifizierung zu verzichten.

Mit Blick auf das in der Informationsgesellschaft notwendige Recht auf anonymes oder hier insbesondere pseudonymes Handeln ist die gerade verabschiedete Regelung der elektronischen Form in § 126a Abs. 1 BGB ein schwerer Fehler. Durch das Erfordernis, den Namen unter die Willenserklärung setzen zu müssen, könnte die Vorschrift datenschutzfeindlich dahingehend ausgelegt werden, dass sie pseudonyme Willenserklärungen ausschließt.[724] Von ihrem Wortlaut her konterkariert sie für formbedürftige Willenserklärungen das Bemühen des Gesetzgebers, pseudonymes Handeln als Möglichkeit des Datenschutzes gerade im Electronic Commerce zu fördern, für den § 126a BGB durch die elektronische Form Erleichterungen bringen soll. Zwischen § 126a Abs. 1 BGB und den Vorschriften in § 3a BDSG, § 4 Abs. 1 TDDSG und § 13 Abs. 1 MDStV besteht ein diametraler Widerspruch. Ob dieser in der Praxis durch eine datenschutzfreundliche Auslegung, die ein aufdeckbares Pseudonym als Name im Sinn von § 12 BGB versteht,[725] beseitigt werden kann, ist alles andere als sicher.[726] Da die geforderte qualifizierte elektronische Signatur ohnehin ein qualifiziertes Zertifikat nach § 7 SigG aufweisen muss, dieses aber auf den Namen oder ein Pseudonym ausgestellt werden kann, sollte statt dem Namen dieses Zertifikat der Erklärung hinzugefügt werden. Entspre-

---

720 S. Teil 3 Kap. 3.4.3.

721 Ebenso *Hoffmann-Riem*, AöR 1998, 532 ff., der sogar Selbstschutz vor staatlichem Datenschutz rangieren lässt.

722 S. hierzu z.B. *Gattung/Grimm/Pordesch/Schneider* 1997, 181; *Schneider/Pordesch*, DuD 1998, 645; *Pordesch*, DuD 1999, 81 ff.; *Federrath/Berthold* 2000, 189.

723 Für *Hoffmann-Riem*, AöR 1998, 532, bringt die informationelle Selbstbestimmung auch eine Verantwortung für den eigenen Selbstschutz mit sich.

724 Hierauf wies die Stellungnahme des *Gesellschaft für Informatik*, DuD 2001, 38, hin.

725 S. hierzu *Roßnagel*, NJW 2001, 1825 unter Hinweis auf Palandt-*Heinrichs*, § 12 Rn. 8.

726 Dies wäre allenfalls für Rollenpseudonyme möglich.

chend einem Vorschlag der Gesellschaft für Informatik[727] sollte § 126a BGB daher datenschutzfreundlich wie folgt gefasst werden:

Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser sein qualifiziertes Zertifikat hinzufügen und das elektronische Dokument zusammen mit dem Zertifikat[728] mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

Der gleiche Fehler deutet sich im Novellierungsverfahren zum VwVfG an. Im Referentenentwurf aus dem Bundesinnenministerium[729] wird in § 3a Abs. 2 Satz 1 VwVfG die elektronische Form mit qualifizierter Signatur nach dem Signaturgesetz der durch Rechtsvorschrift angeordneten Schriftform gleichgesetzt. In Satz 2 wird dann bestimmt: „Die Signatur mit einem Pseudonym ersetzt nicht die Schriftform." Dieser Satz ist ersatzlos zu streichen. Er verträgt sich in keiner Weise mit den Bemühungen um einen modernen Datenschutz.[730] Er sendet das falsche politische Signal. Zudem ist er – auch aus dem Blickwinkel einer um ihre Handlungsfähigkeit besorgten Verwaltung – vollkommen überflüssig.[731] Die in diesem Gutachten vorgeschlagenen Regelungen, um pseudonymes Handeln der Bürger zu ermöglichen, müssen die Verwaltungstätigkeit nicht behindern.[732] Soweit die Verarbeitung personenbezogener Daten nicht erforderlich ist, darf die Verwaltung bereits nach geltendem Recht keine personenbezogenen Daten verarbeiten. Soweit aber eine Rechtsvorschrift die Identifizierung des Bürgers fordert, wird diese weder durch das Erforderlichkeitsprinzip noch durch die Zielvorgabe verhindert, pseudonymes Handeln, soweit möglich und verhältnismäßig, zu ermöglichen. Während eine Streichung des Satzes somit die Verwaltungstätigkeit nicht berührt, wird die Entwicklung eines modernen Datenschutzes, für den das Prinzip der Vermeidung des Personenbezugs eine tragende Säule ist, durch diesen Satz massiv behindert. Im Sinn dieses Prinzips sollte im Zusammenhang mit der anstehenden Novellierung der Datenschutzregelungen in bereichsspezifischen Gesetzen geprüft werden, ob die jeweilige Verwaltungsaufgabe auch bei anonymem Handeln der Bürger in Verbindung mit Garantieerklärungen oder bei Handeln unter Pseudonym erreicht werden kann. Dieser Satz nimmt jedoch das Ergebnis der Prüfung vorweg, bevor sie überhaupt durchgeführt worden ist.

5.2 Infrastrukturverantwortung des Staats

In diesem Kontext wandelt sich die Erfüllungsverantwortung des Staats in eine Infrastrukturverantwortung, die es dem Einzelnen ermöglicht, von den Mitteln des Selbstschutzes Gebrauch zu machen.[733] Zu den Infrastrukturaufgaben gehören:

- rechtliche Absicherungen der individuellen Selbstschutzmöglichkeiten,

---

727 *Gesellschaft für Informatik*, DuD 2001, 38.

728 Dieser Satzteil ist notwendig, um den Zusammenhang zwischen Zertifikat und Erklärung zu schützen. Sie müssen daher beide gemeinsam von der Signatur umfasst werden – S. hierzu *Gesellschaft für Informatik*, DuD 2001, 38; *Roßnagel*, NJW 2001, 1825.

729 Entwurf eines Dritten Gesetzes zur Änderung verwaltungsrechtlicher Vorschriften (3. VwVfÄndG), Stand 30.7.2001.

730 Die Entwurfsbegründung geht mit keinem Wort auf den Widerspruch zu dem bereits geltenden Datenschutzrecht (§ 3a BDSG) ein.

731 Sofern eine pseudonyme Signatur des Behördenvertreters unterbunden werden soll, wird dieses Ergebnis bereits durch die geltende Fassung des § 37 Abs. 3 VwVfG erreicht, erfordert aber jedenfalls nicht, pseudonymes Handeln der Bürger kategorisch auszuschließen.

732 Die Behauptung in der Begründung zu § 3a Abs. 2 Satz 2: „In solchen Fällen lassen sich die mit der Verwendung einer qualifizierten elektronischen Signatur bezweckten Funktionen nicht sicherstellen", trifft nicht zu, wenn ein Aufdeckungsverfahren für Pseudonyme vorgesehen wird – s. hierzu Teil 3 Kap. 5.2.

733 S. hierzu *Roßnagel*, ZRP 1997, 26 ff.; *Hoffmann-Rie*m 1997, 787; *ders*.. AöR 1998, 532, 534; *Vogt/Tauss* 1998, Nr. 9.

- rechtliche Absicherung multilateraler Selbstschutzmöglichkeiten,[734]
- rechtliche Regelungen eines praktikablen und sicheren Aufdeckungsverfahrens für Pseudonyme,
- rechtliche Regelungen zur technisch-organisatorischen Unterstützung von Zahlungsgarantien,
- Aufklärung über Selbstschutzmittel,[735]
- Unterstützung in ihrer Nutzung und
- Förderung und Unterstützung bei der Entwicklung und Gestaltung von Selbstschutzmöglichkeiten.[736]

Eine Infrastrukturaufgabe sind Regelungen für das Angebot und den Umgang mit Pseudonymen. Ohne rechtliche Rahmenregelungen werden sich anonymes und pseudonymes Handeln in der Praxis nicht – zumindest nicht in den für die Verarbeitung personenbezogener Daten relevanten Vertrags- und Verwaltungsbeziehungen – durchsetzen.

Das Recht auf Anonymität und Pseudonymität kann nicht in die Vertragsfreiheit der verantwortlichen Stelle eingreifen. Dieser muss es also grundsätzlich freistehen, ob sie mit einem anonym Handelnden kooperiert.[737]

Eine solche Kooperation ist für sie risikolos, wenn es gleichzeitig zu einem vollständigen Leistungsaustausch kommt oder der anonym Handelnde vorleistet. In beiden Fällen wird sie aber eine vollständige Bezahlung ihrer Leistung fordern und sich mit Bezahlungsverfahren, die nur zu einem Zahlungsversprechen oder zu widerrufbaren Lastschriftmöglichkeiten oder Überweisungsaufträgen führen, nicht zufrieden geben. Ein gleichzeitiger Leistungsaustausch oder gar Vorleistungen des Kunden widersprechen aber den Schutzregelungen, die das Fernabsatzgesetz den Verbrauchern im Electronic Commerce bietet und die diesen beim Fernkauf grundsätzlich eine Prüfung der Ware vor der Bezahlung ermöglichen wollen. Sie werden daher auf Verbraucherseite nur auf geringe Akzeptanz stoßen.

Eine größere Sicherheit für die verantwortliche Stelle könnte durch technisch-organisatorisch unterstützte Zahlungsgarantien erreicht werden, die eine dritte Stelle für einen anonym Handelnden abgibt. Diese wird die Zahlungsgarantie aber nur abgeben, wenn der anonym Handelnde den Betrag bei ihr einzahlt. Die Zahlungsgarantie wird von ihr erst dann eingelöst, wenn der anonym Handelnde die Ware geprüft und die Auszahlung freigegeben hat. Dieses Verfahren führt zu einer Vorleistung der verantwortlichen Stelle, bei der sie vollständig von der Vertrauenswürdigkeit und Fairness der dritten Stelle abhängig ist. Es wird daher wohl nur auf Akzeptanz bei verantwortlichen Stellen stoßen, wenn von Verbraucherseite eine starke Nachfrage nach solchen Vertragsabwicklungsmodellen geltend gemacht wird. Das Vertrauen in solche Verfahren sollte durch gesetzliche Rahmenregelungen gestärkt werden.

Sofern die verantwortliche Stelle auf weiteren Sicherheiten für ihren Zahlungsanspruch besteht, den Partner im Streitfall verklagen können will oder ihn im Normalfall zwar nicht identifizieren, aber wiedererkennen will, weil sie mit ihm eine Beziehung eingeht, die sich nicht in einem einmaligen Leistungsaustausch erschöpft, oder Berechtigungen überprüfen will, bietet sich ein Handeln der betroffenen Person unter Pseudonym an. Kontakte mit der öffentlichen Verwaltung werden in vielen Fällen nicht in anonymer, sondern nur in pseudonymer Form

---

734 S. zu Formen multilateralen Selbstschutzes z.B. *Federrath/Pfitzmann* 1997, 83 ff.; s. hierzu ausführlich Anhang 2, S. 228 ff.

735 S. auch Teil 3 Kap. 4.3.1 am Ende; *Hoffmann-Riem*, AöR 1998, 532, 534.

736 S. auch *Vogt/Tauss* 1998, Nr. 9; *Hoffmann-Riem*, AöR 1998, 532.

737 S. Teil 3 Kap. 5.1.

möglich sein, weil die Verwaltung zumindest im Konfliktfall die Möglichkeit haben muss, die betroffene Person zu identifizieren.[738]

§§ 5 Abs. 3 und 7 Abs. 1 Satz 1 SigG ermöglichen die Ausstellung von Zertifikaten auf ein Pseudonym und damit eine verlässliche und nachprüfbare Form von Pseudonymen. Der Gesetzgeber bietet damit bereits den erforderlichen Kompromiss zwischen der Notwendigkeit der Identifizierung des Handelnden und der Sicherung seiner informationellen Selbstbestimmung, indem diese Pseudonyme ermöglichen, im Ausnahmefall – bei der Verletzung von Rechtspflichten – den Personenbezug des Handelnden über die Zuordnungsregel herzustellen. Pseudonymes Handeln wird an Stelle von anonymem Handeln vor allem deshalb verwendet,[739] weil es die Möglichkeit bietet, im Ausnahmefall die Verantwortung des pseudonym Handelnden geltend zu machen. Da diese Möglichkeit einerseits für viele Anwendungen essentiell ist, zugleich aber leicht missbraucht werden kann, ist eine Regelung notwendig,[740] die einerseits eine Aufdeckung in berechtigten Ausnahmefällen leicht und unbürokratisch ermöglicht, in allen anderen Fällen aber ausschließt.[741] Die Aufdeckung ist auf die zur Rechtsverfolgung notwendigen Angaben zu beschränken.

Ein solches Aufdeckungsverfahren sieht § 14 Abs. 2 SigG bereits vor, allerdings nur für Sicherheitsbehörden, Verfassungsschutzbehörden, Nachrichtendienste und Finanzbehörden. Gerichte können im „Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen" eine Aufdeckung anordnen. Diese Anordnungsbefugnis hilft aber einem klagenden Unternehmen nicht weiter, weil es gegenüber dem Zertifizierungsdiensteanbieter, der über die Zuordnungsliste von Pseudonym zu Identität verfügt, keinen Herausgabe- oder Auskunftsanspruch hat. Wenn aber die allgemeinen Bestimmungen dem Kläger keinen Auskunftsanspruch geben, wird dieser auch nicht durch § 14 Abs. 2 SigG geschaffen. Bevor ein Kläger aber überhaupt zu einer Beweisaufnahme gelangt, in der diese Anordnungsbefugnis eine Rolle spielen könnte, muss er das Problem lösen, wie er zu der ladungsfähigen Anschrift des Beklagten kommt,[742] um überhaupt erst einen Prozess anstrengen zu können.[743] Für Private fehlt ein Aufdeckungsanspruch und ein Aufdeckungsverfahren.[744] Ohne dieses wird pseudonymes Handeln im Electronic Commerce keine Wirklichkeit werden.

An § 14 Abs. 3 SigG könnte etwa folgender Absatz 4 angefügt werden:

Bei einem Signaturschlüssel-Inhaber mit Pseudonym übermittelt der Zertifizierungsdiensteanbieter die Daten über dessen Identität an einen Antragsteller, wenn dieser schriftlich glaubhaft macht, dass die Aufdeckung der Identität unerlässlich ist, um in Gerichts- oder Verwaltungsverfahren eigene Rechte geltend zu machen oder eine durch Gesetz auferlegte Verpflichtung zu erfüllen. Vor der Übermittlung unterrichtet der Zertifizierungsdiensteanbieter den Signaturschlüssel-Inhaber über den Antrag und die Identität des Antragstellers und gibt ihm Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Der Zertifizie-

---

738 In manchen Fällen – wie etwa bei einer Beschwerde – dürfte auch ein selbstaufdeckbares Pseudonym ausreichen, das Rückfragen zulässt, aber nur in vom Nutzer kontrollierten Fällen zu einer Identifizierung führt.

739 Der andere Grund kann die Verkettungsmöglichkeit sein – s. *Roßnagel/Scholz*, MMR 10/2000.

740 S. bereits *provet/GMD* 1994, 210 ff.

741 S. zur Forderung nach einem Aufdeckungsverfahren für Private *Roßnagel*, DuD 1997, 79; *Rieß*, DuD 2000, 533.

742 Dieses Problem stellt sich zumindest solange, bis Prozessordnungen oder Schiedsklauseln netzgestützte Streitentscheidungsverfahren und Formen der Zwangsvollstreckung ohne Kenntnis der physischen Adresse ermöglichen – s. hierzu z.B. *Jung*, K&R 1999, 63.

743 S. hierzu näher *Roßnagel*, NJW 2001, 1821.

744 Zu einem Vorschlag s. bereits *provet*, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gutachten für den BMBF, 1996, http://www.provet.org/bib/mmge oder http://www.iid.de/iukdg/doku.html.

rungsdiensteanbieter kann vom Antragsteller ein Entgelt für die unmittelbar durch die Aufdeckung entstandenen Kosten verlangen.

6. Selbstregulierung

Selbstregulierung ist – neben der Stärkung der Einwilligung[745] – der zweite wichtige Ansatz um im nicht öffentlichen Bereich das Datenschutzrecht zu entlasten und zu verbessern.[746] Daher sollte eine auch von Art. 27 DSRL geforderte Selbstregulierung im vertretbaren Umfang ermöglicht werden, um den jeweiligen Randbedingungen angepasste Datenschutzregelungen zu erreichen. Hierfür muss und kann der Gesetzgeber sich in der inhaltlichen Tiefe seiner Regelungen zurückhalten und die Ausfüllung abstrakter Vorgaben der Selbstregulierung überlassen. Die schnelle Entwicklung der Technik, die Komplexität ihrer Systeme und die Vielfalt ihrer Anwendungen lässt es ihm angeraten sein, sich hinsichtlich detaillierter Regelungen zurückzuhalten. Selbstregulierung ermöglicht es der Wirtschaft, relativ schnell passgerechte branchen- oder unternehmensbezogene Regelungen zu entwickeln, die insbesondere auch eine globalisierte Datenverarbeitung vereinfachen, wenn diese Regelungen weltweite Anwendung finden. Der entscheidende Anreiz für Branchen, Verbände oder Unternehmen, eigene, durch Kontrollstellen anerkannte Verhaltensregeln zu erstellen, besteht in der Möglichkeit, die zu konkretisierenden Gesetzesvorgaben selbständig auszugestalten, für die Geltungsdauer der Regelungen über fest umrissene, klare Rahmenbedingungen der Datenverarbeitung zu verfügen und in diesem Rahmen nicht der Auslegungsprärogative der Kontrollstellen auf Grundlage der gesetzlichen Regelungen zu unterliegen.

Selbstregulierung entspricht dem Prinzip der Kooperation zwischen Staat und Gesellschaft.[747] Sie wird insbesondere für die vielfältigen Probleme des elektronischen Handelns von der Europäischen Union als Regelungsprinzip bevorzugt.[748] Für den Bereich des Datenschutzes haben auch andere Rechtsordnungen Selbstregulierungsmechanismen vorgesehen. Unter Berücksichtigung der dort gemachten – unterschiedlichen – Erfahrungen[749] sollte Selbstregulierung nach folgenden Regeln zugelassen und gefördert werden.

6.1 Konkretisierende und ergänzende Selbstregulierung

Selbstregulierung soll und kann nicht als Ersatz für rechtlichen Datenschutz stehen, sondern sollmit diesem gemeinsam die Herausforderungen des Datenschutzes arbeitsteilig bewältigen.

---

745 S. Teil 3 Kap. 3.1 und 3.3.

746 S. zur Selbstregulierung im Datenschutz z.B. *Swire* 1997; *Perritt* 1997; *Merold* 1997; *Mayen*, NVwZ 1997, 446, 450; *Trute*, VVDStRL 57 (1998), 262f.; *Vogt/Tauss* 1998, Nr. 16; *Bizer*, DuD 1999, 7 ff.; *Ladeur*, DuD 2000, 15 ff.; *Heil*, DuD 2001, 129 ff.; *Büllesbach/Höss-Löw*, DuD 2001, 135 ff.; *Nitsche*, DuD 2001, 164 ff.; *Kranz*, DuD 2001, 161 ff.; *Karstedt-Meierrieks*, DuD 2001, 287 ff.

747 Im Kontext der Europäischen Gesetzgebung wird von Selbstregulierung ein bedeutender Beitrag erwartet, wenn es um öffentliche Interessen hinsichtlich des Inhalts von Informationsangeboten wie etwa beim Jugendschutz oder der Werbung geht. Als weniger geeignet wird diese Regulierungsform angesehen, wenn es um Wettbewerbsfragen oder um das Verfolgen kultureller, politischer oder sozialer Ziele geht. S. Europäische Kommission Ergebnisse der öffentlichen Konsultation zum Grünbuch „Die Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihre ordnungspolitischen Auswirkungen" vom 10.3.1999, KOM(1999)108; Europäische Kommission, eEurope 2002 – Eine Informationsgesellschaft für alle – Aktionsplan, vorbereitet von Rat und Europäische Kommission zur Vorlage auf der Tagung des Europäischen Rates am 19./20. Juni in Feira, 14.6.2000, 19f., http://europa.eu.int/comm/ information_society/eeurope/documentation/index_de.htm.

748 Zur Rolle der Selbstregulierung s. auch die Initiative „e-Europe 2002", Europäische Kommission, eEurope 2002 – Eine Informationsgesellschaft für alle – Aktionsplan, vorbereitet von Rat und Europäische Kommission zur Vorlage auf der Tagung des Europäischen Rates am 19./20. Juni in Feira, 14.6.2000, 19f., http://europa.eu.int/comm/information_society/eeurope/documentation/index_de.htm.

749 S. hierzu z.B. *Overkleeft-Verburg* 1996, 41 ff.; *Kuitenbrouwer* 1997; *U.S. Department of Commerce* 1997; *Roßnagel* 2000b, 385; *Grimm/Roßnagel*, DuD 2000, 446; *Roßnagel/Scholz*, DuD 2000, 454 ff.

Daher sollte der demokratisch legitimierte Gesetzgeber grundsätzliche Regeln und einen Verfahrensrahmen schaffen, innerhalb dessen Wirtschaftsverbänden, Berufsverbänden oder sonstigen Vereinigungen (im Folgenden „Verbände“) wie auch einzelnen Unternehmen die Chance eröffnet wird, spezifische Verhaltensregelungen zu treffen.

Eine gesetzesersetzende Selbstregulierung wäre im Bereich des Datenschutzrechts verfassungswidrig, soweit Eingriffe in das Grundrecht auf informationelle Selbstbestimmung geregelt werden, die einer gesetzlichen Erlaubnis bedürfen. Sie wäre auch europarechtswidrig, weil die Umsetzung der DSRL eine verbindliche und einklagbare gesetzliche Regelung fordert. Selbstregulierung kann daher nur in Ausfüllung solcher Regelungen erfolgen.[750]

Die Verbände sollten die gesetzlichen Grundsatzregelungen konkretisieren, ausfüllen oder ergänzen, aber nicht einschränken können.[751] Die mit diesem Ziel erarbeiteten Verhaltensregelungen sind danach die Fortsetzung eines vom Gesetzgeber eingeleiteten und gestalteten Regelungsprozesses. Sie verstärken die Regelungstiefe der gesetzlichen Vorgaben und tragen den Besonderheiten der jeweiligen Branche Rechnung.[752] Die gesetzlichen Regelungen dienen dabei als Anleitung für die Erstellung der Verhaltensregeln. Sie sind zugleich die eng auszulegende normative Rückfallposition, wenn Selbstregulierung misslingt oder deren Ergebnisse von verantwortlichen Stellen nicht angenommen werden.[753]

Gegenstand der Selbstregulierung könnten zum Beispiel sein:

- die Konkretisierung des Erlaubnistatbestands „eigene Rechte oder Rechte Dritter zu verfolgen oder zu schützen“,[754]
- die Konkretisierung der Erforderlichkeit bestimmter Daten für bestimmte Zwecke,
- die brancheneinheitliche Festlegung notwendiger Vertragsdaten und des Angebots zivilisatorischer Grundleistungen ohne zusätzliche Datenverarbeitung,[755]
- die Konkretisierung und Abgrenzung von Zweckbestimmungen,
- Grundsätze für die branchenspezifische Unterrichtung betroffener Personen,[756]
- die Konkretisierung der Ausnahmegründe für die Unterrichtung, wenn die Datenerhebung nicht bei der betroffenen Person erfolgt,[757]
- branchenspezifische Datenschutzerklärungen,[758]
- Konkretisierung branchenspezifischer Verfahren anonymen und pseudonymen Handelns,[759]
- Konkretisierung branchenspezifisch notwendiger Sicherungsmaßnahmen,[760]

---

750 S. Teil 3 Kap. 5.8.

751 S. hierzu auch das Beispiel der Selbstregulierung der Datenverarbeitung für journalistische Zwecke nach dem italienischen Datenschutzgesetz – s. zu dem Beispiel *Simitis*, DuD 2000, 724.

752 Ebenso *Simitis*, DuD 2000, 724.

753 S. Teil 3 Kap. 6.5.

754 S. Teil 3 Kap. 3.1.

755 S. Teil 3 Kap. 3.3.1.

756 S. Teil 3 Kap. 3.2.1.

757 S. Teil 3 Kap. 3.2.2.

758 S. Teil 3 Kap. 3.2.3; s. hierzu auch z.B. die Datenschutzerklärung des Arbeitskreises „Datenschutzaudit Multimedia“, DuD 1999, 285; s. hierzu auch ausführlich *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4, Rn. 52 ff.

759 S. Teil 3 Kap. 3.4.3.

760 S. Teil 3 Kap. 3.6.

- die Einrichtung branchenspezifischer Schlichtungsverfahren[761] an Stelle oder als „zweite Instanz“ zur Beschwerdemöglichkeit gegenüber dem betrieblichen Datenschutzbeauftragten[762] oder
- die Erarbeitung brancheneinheitlicher Einwilligungserklärungen.[763]

Über diese Beispiele hinaus sollte es den Verbänden freistehen, die gesetzlichen Regelungen zu konkretisieren, für die sie einen praktischen Konkretisierungsbedarf sehen.

Indem der Gesetzgeber nicht alle Details selbst entscheidet, sondern die Kooperation mit den verarbeitenden Stellen sucht, bietet er ihnen die Chance, die gesetzlichen Anforderungen aufzugreifen und im Hinblick auf die eigenen Aktivitäten zu präzisieren.[764] Dabei könnten die Datenschutzerklärungen der einzelnen Unternehmen der Ausgangspunkt für die Erarbeitung branchenspezifischer Verhaltensregeln sein.[765]

6.2 Anreize zur Selbstregulierung und Zielfestlegungen

Staat und Gesetzgeber sollten Selbstregulierung fördern und für ihre Durchführung vertretbare Anreize schaffen.

Der wesentliche Anreiz für die verantwortlichen Stellen, sich an der Selbstregulierung zu beteiligen, ist die Möglichkeit, nach den in Kap. 6.4 und 6.5 beschriebenen Regeln auch für die Kontrollstellen verbindliches Recht zu setzen. Für die verantwortlichen Stellen kann es einen entscheidenden Unterschied in der Praxis der Datenverarbeitung machen, ob sie Begriffe wie „Erforderlichkeit“, „Vereinbarkeit mit dem Verarbeitungszweck“, „Angebot anonymer und pseudonymer Nutzungsmöglichkeiten“ oder „ausreichende Sicherheitsmaßnahmen“ selbst branchenspezifisch präzisieren können oder ob dies durch die Kontrollstellen erfolgt. Haben die Kontrollstellen nach dem in Kap. 6.4 beschriebenen Verfahren die selbstgesetzten Verhaltensregeln als mit dem Datenschutzrecht vereinbar anerkannt, sind auch sie an diese Regeln gebunden.[766] Im Gesetz sollte aus Gründen des Vertrauensschutzes ausdrücklich klargestellt werden, dass die Kontrollstellen gegenüber abschließenden Regelungen in anerkannten Verhaltensregelungen keine weitergehenden Anforderungen stellen können.[767] Diese Bindung begrenzt zwar die Flexibilität der Kontrollstellen, ist in ihrer faktischen Auswirkung allerdings wiederum dadurch beschränkt, dass die Anerkennung einer Verhaltensregel zeitlich auf maximal fünf Jahre befristet ist.[768] Diese Regelung ermöglicht einen akzeptablen Kompromiss zwischen Anreiz zur Selbstregulierung durch behördliche Bindung und Flexibilität der Gesetzeskonkretisierung durch zeitliche Befristung der Anerkennung.

Ein weiterer Anreiz zur Selbstregulierung oder zu freiwilligen Maßnahmen zur Förderung von Datenschutz und Datensicherheit kann das Instrument der *Zielfestlegungen* bieten. Mit diesem wird vor einer gesetzlichen Festlegung von Anforderungen den interessierten Kreisen die Gelegenheit geboten, das Regelungsziel durch freiwillige Maßnahmen zu erreichen.

Das Gesetz sollte der Bundesregierung die Möglichkeit bieten, für die freiwillige Erfüllung von Anforderungen zur Vorsorge gegen Risiken für die informationelle Selbstbestimmung

---

761 S. zum japanischen Recht, zu den Safe Harbor Principles und zum niederländischen Datenschutzgesetz Teil 3 Kap. 6.4.

762 S. hierzu Teil 3 Kap. 6.4.

763 S. Teil 3 Kap. 3.3.4.

764 Ebenso *Simitis*, DuD 2000, 724.

765 So für den Luftverkehr *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4 Rn. 53.

766 S. Teil 3 Kap. 5.6.

767 Eine vergleichbare Regelung schlug § 36 Abs. 3 des Entwurfs eines UGB vor – s. zur Begründung UGB-KOM-E 1998, 511.

768 S. Teil 3 Kap. 6.4.

formell Zielfestlegungen zu treffen, die innerhalb einer bestimmten Frist erreicht werden sollen. Das Gesetz sollte weiter festlegen, dass die Bundesregierung, wenn die festgelegten Ziele innerhalb der vorgegebenen Frist nicht erreicht werden, zu prüfen hat, welche gesetzgeberischen Maßnahmen zu ergreifen sind, um die Ziele durch Rechtsvorschriften zu erreichen.

Das Instrument der Zielfestlegung entstammt dem Abfallrecht, wurde dort erstmals 1986 mit der Novellierung des Abfallgesetzes durch § 14 Abs. 2 Satz 1 AbfG eingeführt und findet sich heute in § 25 Abs. 1 KrW-/AbfG.[769] Die Bundesregierung hat bisher zweimal von diesem Instrument Gebrauch gemacht[770] und Entwürfe für vier weitere Zielfestlegungen vorbereitet, sie aber nicht verabschiedet. Die Ansichten über die praktische Bewährung von Zielfestlegungen gehen auseinander. Dennoch überwiegen in der Literatur die Stimmen, die die Zielfestlegung für ein rechtspolitisch interessantes Instrument halten, das sich als „formalisierte Drohgebärde“[771] positiv auf das Verhalten der betroffenen Wirtschaftskreise auswirkt, indem es ihnen die Möglichkeit einräumt, zunächst selbst zu bestimmen, mit welchen Mitteln die jeweiligen Ziele erreicht werden sollen.[772] Aus diesem Grund sieht auch der Entwurf für ein UGB in § 34 Zielfestlegungen vor.[773]

Das Instrument der Zielfestlegung ist auch zur Förderung von Datenschutz und Datensicherheit geeignet, weil es erlaubt, vor allem für die Technikentwicklung und -gestaltung mittelfristig Ziele vorzugeben, die verbindlich zu regeln gegenwärtig unmöglich wäre, weil die Informations- und Kommunikationstechnik sie nicht oder nicht mit verhältnismäßigen Mitteln umzusetzen erlaubt. Geeignete Zielfestlegungen könnten zum Beispiel darin bestehen, innerhalb einer bestimmten Frist für bestimmte Anwendungsfelder

- den Einsatz von Systemen mit offengelegten Quelltexten vorzusehen,[774]
- die technische Kennzeichnung von Verarbeitungszwecken und deren technische Kontrolle zu fordern,[775]
- die Unterstützung der informationellen Gewaltenteilung durch getrennte Datenverarbeitung vorzusehen,[776]
- die Verwendung von Betriebssystemen zu fordern, die geschützte und kontrollierte Verarbeitungsbereiche bieten,[777]
- den Aufbau eines Netzes von Beratungsstellen zu fordern, in denen Beratungsgutscheine aus dem Erwerb eines Produkts der Informations- und Kommunikationstechnik eingelöst werden können,[778]
- spezifische Anforderungen an künftige Produkte der Informationstechnik zu stellen[779] oder

---

769 S. hierzu sowie zu Literaturnachweisen UGB-KOM-E 1998, 502.

770 Zielfestlegung der Bundesregierung zur Vermeidung, Verringerung und Verwertung von Abfällen aus Verpackungen für Getränke vom 26.4.1989, BAnz vom 6.5.1989, 2237, und Zielfestlegung der Bundesregierung zur Vermeidung, Verringerung und Verwertung von Abfällen von Verkaufsverpackungen aus Kunststoff für Nahrungs- und Genussmittel sowie Konsumgüter vom 17.1.1990, BAnz vom 30.1.1990, 513.

771 *Jekewitz*, DÖV 1990, 57.

772 S. weitere Hinweise in UGB-KOM-E 1998, 502.

773 S. zur Begründung UGB-KOM-E 1998, 502 und 508f.

774 S. Teil 3 Kap. 3.2.6.

775 S. Teil 3 Kap. 3.5.7.

776 S. Teil 3 Kap. 3.5.7.

777 S. Teil 3 Kap. 3.5.7.

778 S. Teil 3 Kap. 4.3.1.

779 S. Teil 3 Kap. 4.3.1.

- die Möglichkeit einer automatisierten Online-Einsicht in die Daten der betroffenen Person zu fordern.[780]

Für die Technikhersteller und die verantwortlichen Stellen gibt die Zielfestlegung einen politisch klaren Rahmen für ihre Investitionsentscheidungen vor. Sie haben die Möglichkeit, durch Koordination ihrer Aktivitäten eine spätere rechtliche Verpflichtung überflüssig zu machen und sich so größere Handlungsspielräume zu erhalten. Gelingt ihnen eine solche Koordination nicht oder sind sie an einer freiwilligen Umsetzung des Ziels nicht interessiert, haben sie zumindest den Vorteil, dass sie sich mittel- oder längerfristig auf die künftige Regelung einstellen können.

Der Bundesregierung ermöglicht das Instrument der Zielfestlegung, Prioritäten zu setzen und die Richtung ihrer Politik zu bestimmen. Die Zielfestlegung wirkt entweder normvermeidend, wenn die Ziele freiwillig erfüllt werden und dadurch auf weitere Regulierungen verzichtet werden kann, oder sie wirkt normvorbereitend, indem sie die künftigen Regelungsadressaten bereits auf die Regelung „einstimmt".

Für die Allgemeinheit hat dieses Verfahren den Vorteil, dass „politischer Druck" zur Förderung von Datenschutz und Datensicherheit entfaltet wird. Die Zielfestlegung kann sich auf Forderungen erstrecken, die gegenwärtig nicht in einer verbindlichen Regelung umgesetzt werden könnten. Insofern können durch Zielfestlegungen Fortschritte in Datenschutz und Datensicherheit in die Zukunft hinein strukturiert werden. Die Prüfungspflicht der Bundesregierung nach Ablauf der Zielerreichungsfrist soll sicherstellen, dass gebotene Rechtsvorschriften umgesetzt werden oder Rechenschaft darüber abgelegt wird, warum trotz Zielverfehlung die Rechtsvorschriften entbehrlich sind. Dieses Verfahren führt zu einer Stärkung politischer Rationalität.

Zielfestlegungen sind keine Rechtsnormen, sondern primär politische Akte, die eine gewisse zeitlich begrenzte politische Selbstbindung der Bundesregierung bewirken, darüber hinaus aber keine rechtlichen Wirkungen entfalten. Sie können jedoch eine beträchtliche faktische Wirkung erzeugen, die dadurch verstärkt wird, dass die Nichtbefolgung der Zielfestlegung durch den Erlass entsprechender Regelungen „sanktioniert" wird.[781]

Gegenstand der Zielfestlegung können nur Vorsorgemaßnahmen sein, nicht jedoch Maßnahmen, die zum unmittelbaren Schutz der informationellen Selbstbestimmung erforderlich sind. Für solche Maßnahmen würde ein Vertrauen auf das freiwillige Verhalten verantwortlicher Stellen der staatlichen Schutzpflicht zuwiderlaufen.

Eine Regelung, um Zielfestlegungen zu ermöglichen, könnte etwa folgenden Wortlaut haben:

(1) Die Bundesregierung kann für die freiwillige Erfüllung von Anforderungen zur Vorsorge gegen Risiken für die informationelle Selbstbestimmung Zielfestlegungen treffen, die innerhalb einer bestimmten Frist erreicht werden sollen. Die Zielfestlegungen sind in geeigneter Weise öffentlich bekannt zu machen.

(2) Wenn nach Absatz 1 festgelegte Ziele innerhalb der vorgegebenen Frist nicht erreicht werden, prüft die Bundesregierung, welche gesetzgeberischen Maßnahmen zur Erreichung der Ziele zu ergreifen sind. Die Befugnis, auch vor Ablauf der vorgegebenen Frist Maßnahmen zu treffen, bleibt unberührt.

[780] S. Teil 3 Kap. 7.1.3.

[781] S. hierzu auch UGB-KOM-E 1998, 508.

6.3 Regulierte Selbstregulierung

Auch für die Selbstregulierung gilt, dass sie die Grundrechte Dritter betrifft. Die Schutzaufgabe des Staats erstreckt sich damit auch auf diesen Bereich und er kann sie weder inhaltlich noch verfahrensmäßig vollständig den interessierten Kreisen überlassen. Vielmehr muss der Gesetzgeber Regeln für die Selbstregulierung treffen. Zulässig ist im Datenschutzrecht eine verbindliche[782] Regulierung nur dann, wenn sie auf einer gesetzlichen Grundlage aufbaut. Diese Regelungen für die Selbstregulierung müssen nicht umfangreich sein.

Selbstregulierung dient der Entlastung des Datenschutzrechts und eröffnet der Wirtschaft Möglichkeiten, an der Gestaltung des Datenschutzrechts mitzuwirken. Um passgerechte, weitreichende und überschaubare Regelungen zu finden, sollten sowohl Unternehmen wie auch Verbände Adressaten der gesetzlichen Vorgaben sein. Dabei sind folgende praxisrelevante Konstellationen zu beachten:

In den Fachgesprächen zu diesem Gutachten wurden vielfach Zweifel geäußert, ob kleine und mittlere Unternehmen an eigenständiger Selbstregulierung interessiert seien und den Aufwand, der mit der Aufgabe der Selbstkoordinierung von Konkurrenten verbunden ist, erbringen könnten. Selbstregulierung ist in der Tat auch immer eine Frage einer Kosten-Nutzen-Rechnung. Insbesondere kleinere Unternehmen sind hier auf die Vorarbeit ihrer Verbände angewiesen. Zugleich ist es für sie wichtig, dass für die Selbstregulierung der unterschiedliche Handlungsrahmen für kleine und mittlere Unternehmen einerseits und Großunternehmen andererseits berücksichtigt werden kann. Im Bereich der kleinen und mittleren Unternehmen wird es – wenn überhaupt – wohl nur zu einer Selbstregulierung durch Verbände kommen.

Umgekehrt zielen weltweit tätige Unternehmen auf eine weltweite Geltung ihrer Selbstregulierung. Für sie ist der Rahmen des nationalen Wirtschaftsverbands viel zu eng. In manchen Märkten gibt es nur ein einziges nennenswertes Unternehmen in der Bundesrepublik Deutschland. In diesen Fällen besteht kein Interesse oder auch keine Möglichkeit einer Branchenregelung. Daher sollte es auch möglich sein, dass ein einzelnes Unternehmen, das sich selbst verbindliche Regeln setzt, an den Selbstregulierungsverfahren teilnehmen kann.[783]

Soll Selbstregulierung ermöglicht werden, muss aber zweierlei beachtet werden: Zum Einen darf sie nicht zu einer Rechtszersplitterung führen. Diesem Ziel dienen die gesetzlichen Rahmenvorgaben. Die inhaltliche Anleitung erfolgt dadurch, dass die Selbstregulierung die oft sehr allgemein bleibenden gesetzlichen Regelungen präzisieren, aber nicht verändern darf.

Zum Anderen ist der Interessenselektivität jeder Selbstregulierung entgegen zu wirken. Diese ergibt sich vor allem dadurch, dass in der Selbstregulierung noch stärker als in anderen Regelungsformen sich spezielle Interessen leichter organisieren lassen als allgemeine Interessen, aktuelle Interessen sich leichter durchsetzen lassen als langfristige und zukünftige Interessen und dass wirtschaftliche Interessen den sozialen, kulturellen, persönlichen und anderen nichtökonomischen Interessen in der Praxis vorgehen. Für das Verfahren der Selbstregulierung sind Regelungen notwendig, die ein Mindestmaß an Fairness und Interessenberücksichtigung gewährleisten. Aus diesem Grund fordert die Europäische Kommission, dass bei jeder Verabschiedung und Anwendung von Selbstregulierungsmaßnahmen die Verbraucher „voll einbezogen werden“.[784] Ähnliche Anforderungen enthalten zum Beispiel Art. 25 Abs. 3 des

---

[782] Unverbindliche Selbstregulierung bedarf keinen regelnden Vorgaben, sondern ist Angelegenheit der Beteiligten. Auch zu ihr sollten staatliche Stellen ermuntern.

[783] Auch § 35 Abs. 1 des Entwurfs eines UGB sieht die Möglichkeit von Selbstverpflichtungen für einzelne Unternehmen vor.

[784] Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft „Informationen des öffentlichen Sektors – eine Schlüsselressource für Europa“, KOM(1998)585, 26.

niederländischen Datenschutzgesetzes[785] und Art. 31 Abs. 1 h) des italienischen Datenschutzgesetzes.[786]

Die Selbstregulierung sollte auf einen gesellschaftlichen Konsens, nicht auf die einseitige Durchsetzung der Interessen eines Verbands zielen. Daher sollten sich anerkannte Datenschutz- und Verbraucherverbände an der Selbstregulierung beteiligen können.[787] Verbraucherverbände werden nach § 22a AGBG vom Bundesverwaltungsamt anerkannt, wenn es sich um rechtsfähige Vereine mit mehr als 75 Mitgliedern handelt, „die Interessen der Verbraucher durch Aufklärung und Beratung wahrnehmen". Datenschutzverbände könnten nach den gleichen Kriterien anerkannt werden, hierfür wäre in § 22a AGBG nur eine kleine Ergänzung vorzusehen: Nach dem Wort „Verbraucher" wäre „und der von der Datenverarbeitung Betroffenen" einzufügen.

Um eine sinnvolle Beteiligung dieser Verbände zu gewährleisten, ist eine ausreichende Transparenz und Interessenartikulation zu gewährleisten. Der regelsetzende Verband oder das regelsetzende Unternehmen sollte die Verbraucher- und Datenschutzverbände über ihr Vorhaben, ihre Entwürfe und ihre Ergebnisse informieren. Die Verbraucher- und Datenschutzverbände sollten die Möglichkeit haben, zu den Entwürfen Stellung zu nehmen und um eine Anhörung nachzusuchen. Der Nachweis, dass ihnen Gelegenheit zur Stellungnahme gegeben worden ist, sollte eine formale Voraussetzung für die Anerkennung der Verhaltensregel sein.

Diese zwingende Form der Zusammenarbeit bringt für die Verbände oder Unternehmen den Vorteil mit sich, in der Anerkennung ihrer Regeln auf einen Konsens mit den Verbraucher- und Datenschutzverbänden verweisen zu können. Andernfalls müssen sie mit Widerständen rechnen, wenn sie diesen Konsens nicht gesucht haben. Für die Kontrollstellen besteht der Vorteil, dass sie nicht allein die Interessen der betroffenen Personen vertreten müssen, sondern eher in die Rolle eines Schiedsrichters gelangen, der dadurch „stabilisiert wird, dass er von beiden Seiten Druck erfährt".

Die Regelung zur Erstellung von Verhaltensregeln könnte etwa wie folgt lauten:

(1) Verantwortliche Stellen oder Vereinigungen von verantwortlichen Stellen können Verhaltensregeln zur Präzisierung, Ausgestaltung oder Erweiterung von datenschutzrechtlichen Anforderungen erstellen.

(2) Das Verfahren zur Erstellung der Verhaltensregeln muss demokratischen Grundsätzen entsprechen, öffentlich bekannt gemacht werden und allen, die von den Verhaltensregeln betroffen sein können, die Möglichkeit einräumen, ihre Interessen zum Ausdruck zu bringen.

(3) Nach § 22a des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen anerkannten Vereinen, die Interessen der Verbraucher oder der von der Datenverarbeitung betroffenen Personen wahrnehmen, ist Gelegenheit zu geben, zum Entwurf der Verhaltensregeln Stellung zu nehmen.

6.4 Anerkennung der selbstgesetzten Regeln

Um das demokratische Defizit der Selbstregulierung auszugleichen und die Zielerreichung sicherzustellen, sind die Ergebnisse der Selbstregulierung entsprechend Art. 27 Abs. 2 DSRL

---

785 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

786 Gesetz Nr. 675 vom 31.12.1996.

787 So auch z.B. *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4 Rn. 54: Für die Branche wäre dies ein „weiterer greifbarer Beleg für ihre deutliche Kundenorientierung". Er geht davon aus, dass im Sinn zivilgesellschaftlicher Einflußnahme auf sozial relevante Prozesse künftig der Einfluss von Konsumentenorganisationen weltweit deutlich zunehmen wird. Insofern rechtfertigen sich für ihn solche Bestrebungen nicht etwa lediglich aus allgemeinen wirtschaftsethischen oder philanthropischen Motivationen sondern eher und im Besonderen auch aus Gründen rational fundierter ökonomisch orientierter Planung der Geschäftsprozesse.

von zuständigen staatlichen Organen auf ihre Vereinbarkeit mit dem Datenschutzrecht zu überprüfen und anzuerkennen.[788] Dafür sollten die Kontrollstellen zuständig sein.[789] Entsprechend der gegebenen Verwaltungskompetenz im Datenschutzrecht bietet es sich an, dass für die Anerkennung die Kontrollstelle des Bundeslands zuständig ist, in der das Unternehmen oder der Verband, der die Verhaltensregeln anmeldet, seinen Sitz hat. Für Unternehmen oder Verbände mit Sitz im Ausland sollte der BfD zuständig sein.

Die Anerkennung der selbstgesetzten Verhaltensregeln sollte zeitlich befristet sein, um eine Neuüberprüfung nach einem gewissen Zeitablauf zu ermöglichen. Hierfür wird eine Frist von höchstens fünf Jahren vorgeschlagen.[790] Bei der Neuanerkennung sind Änderungen in der Datenverarbeitung, in den Risiken für die geschützten Grundrechte und in der Abschätzung der künftigen Entwicklung in dem neuen Anerkennungszeitraum zu berücksichtigen.

Anerkannte Verhaltensregeln sollten im jeweils zuständigen Amtsblatt veröffentlicht werden.[791] Dies entspricht den Publizitätsanforderungen an verbindliche[792] Rechtsregelungen.[793] Nicht nur die betroffenen verantwortlichen Stellen, sondern auch alle betroffenen Personen müssen in der für Rechtsnormen üblichen Weise erfahren können, welche Datenschutzregelungen in einer bestimmten Branche verbindlich sind. Zusätzlich sollte der Verband, der die Regeln gesetzt hat, jedes beigetretene Unternehmen sowie die zuständige Kontrollstelle die Regeln im Internet verfügbar halten. Für die verantwortlichen Stellen, die im elektronischen Geschäftsverkehr tätig sind, muss diese Pflicht entsprechend Art. 10 Abs. 2 der Electronic-Commerce-Richtline ohnehin geschaffen werden. Danach müssen Diensteanbieter alle einschlägigen Verhaltenskodizes, denen sie sich unterwerfen, einschließlich Informationen darüber, wie diese Kodizes auf elektronischem Weg zugänglich sind, im Internet angeben.

Wenn die Verhaltensregeln möglichst weltweite oder zumindest europaweite Geltung haben sollten, müssten sie weltweit oder europaweit anerkannt sein. Hierfür wäre anzustreben, dass nur eine Kontrolle und Anerkennung erforderlich ist. Dies kann von der Bundesrepublik Deutschland aus für die weltweite Anerkennung nur angeregt, für den Rechtsraum der Europäischen Gemeinschaft als Regelungsentwurf vorgeschlagen werden.

Für den Rechtsraum der Europäischen Gemeinschaft könnte allerdings bereits ausreichen, wenn die Verhaltensregel in der Bundesrepublik Deutschland anerkannt ist. Denn die Datenverarbeitung ist nach Art. 4 DSRL europaweit zulässig, wenn sie in dem Mitgliedstaat zulässig ist, in dem die verantwortliche Stelle ihren Sitz hat. Dieses Sitzlandprinzip gilt umgekehrt nach § 1 Abs. 4 BDSG bereits heute auch für die Datenverarbeitung, für die die Rechtsordnung eines anderen Mitgliedstaats ausschlaggebend ist.

In ähnlicher Weise wirkt die Anerkennung einer Verhaltensregel durch die Kontrollstelle eines Bundeslands für das gesamte Bundesgebiet. Der Verwaltungsakt eines Landes im Vollzug von Bundesgesetzen enthält rechtliche Festsetzungen – hier eine Feststellungswirkung –, die

---

788 S. auch *Kranz*, in: *Roßnagel*, HB-Datenschutzrecht, Kap. 7.4 Rn. 53.

789 S. auch *Simitis*, DuD 2000, 724.

790 Dies entspricht Art. 25 Abs. 5 des Niederländischen Datenschutzgesetzes, Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302, und § 36 Abs. 1 Nr. 4 des Entwurfs für ein UGB, der für normersetzende Verträge eine Geltungsdauer von ebenfalls höchstens fünf Jahren vorsieht.

791 Ebenso Art. 25 Abs. 4 des Niederländischen Datenschutzgesetzes, Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

792 S. zur Verbindlichkeit differenziert Teil 3 Kap. 6.5.1.

793 Der Entwurf für ein UGB fordert aus diesem Grund in § 36 Abs. 1 Satz 4 für normersetzende öffentlich-rechtliche Verträge, die für das Umweltrecht insofern eine vergleichbare Wirkung haben, die Veröffentlichung im Bundesanzeiger – s. auch UGB-KOM-E 1998, 511.

als solche überall im Bundesgebiet beachtet werden müssen.[794] Eine ausdrückliche gesetzliche Regelung ist hierfür nicht erforderlich.

Etwas anderes gilt nur, wenn die Verhaltensregeln – wie Tarifverträge – nicht bundeseinheitlich von den jeweiligen Spitzenverbänden, sondern mit regional begrenztem Geltungsbereich erstellt werden. Dann gilt die Verhaltensregel nur in dem vorgesehenen Geltungsbereich. In diesem Fall müsste sie, wenn sie von einem anderen Verband mit einem anderen Geltungsbereich übernommen wird, erneut anerkannt werden.

Die Vorschrift zur Anerkennung von Verhaltensregeln könnte etwa folgenden Wortlaut haben:

(1) Die zuständige Kontrollstelle stellt auf Antrag innerhalb von drei Monaten die Vereinbarkeit der Verhaltensregeln mit dem geltenden Recht fest. Mit dem Antrag sind die Darstellung des Erstellungsverfahrens sowie eingegangene Stellungnahmen, insbesondere die von nach § X Abs. 3[795] zu beteiligenden Vereinen, vorzulegen. Die Feststellung nach Satz 1 ist zu befristen und darf nicht länger als für eine Frist von fünf Jahren gelten. Für Stellen oder Vereinigungen mit Sitz im Ausland ist der Bundesbeauftragte für den Datenschutz zuständig.

(2) Anerkannte Verhaltensregeln werden im zuständigen Amtsblatt und in geeigneter Weise von der Kontrollstelle sowie der Vereinigung oder der verantwortlichen Stelle veröffentlicht.

(3) Verhaltensregeln sind für eine verantwortliche Stelle und im Verhältnis zu ihr für die Kontrollstellen für die Dauer der Feststellung nach Absatz 1 verbindlich, wenn sich die verantwortliche Stelle gegenüber der zuständigen Kontrollstelle schriftlich zu ihrer Einhaltung verpflichtet.

(4) Die Kontrollstelle führt ein öffentliches Register der ihr gegenüber erklärten Verpflichtungen. Sie übermittelt am Ende eines jeden Jahres ein fortgeschriebenes Verzeichnis der registrierten Verpflichtungen an den Bundesbeauftragten für den Datenschutz, der das Verzeichnis der Öffentlichkeit zugänglich macht.

Das Niederländische Datenschutzgesetz[796] fordert in Art. 25 Abs. 4, dass die Entscheidung über die Anerkennung der Verhaltensregeln innerhalb einer angemessenen Frist, spätestens nach 13 Wochen, getroffen werden. Eine vergleichbare Regelung sollte auch in Deutschland vorgesehen werden.

6.5 Freiwillige, aber verbindliche Geltung

Für drei Bereiche – Datenschutz in der Forschung, in der journalistisch-literarischen Arbeit sowie in Warndiensten, Detekteien und Auskunfteien – soll die Selbstregulierung verpflichtend sein.[797] Die Befolgung dieser Pflicht soll dadurch durchgesetzt werden, dass die allgemeinen (für die verantwortliche Stelle eher ungünstigen, weil nicht von ihr selbst präzisierten) Datenschutzregeln solange gelten, bis die Verbände eigene anerkannte Verhaltensregeln geschaffen haben. Ansonsten aber ist das Aufstellen von Verhaltensregeln den Verbänden freigestellt.

---

[794] S. z.B. BVerfGE 11, 6 (19): Es liege im Wesen des landeseigenen Vollzugs von Bundesgesetzen, dass der zum Vollzug eines Bundesgesetzes ergangene Verwaltungsakt eines Landes grundsätzlich im ganzen Bundesgebiet Geltung hat. Für dieses Ergebnis spielt es keine Rolle, ob es mit einer Gleichsetzung von Geltungsbereich eines Aktes der Verwaltung mit dem Geltungsbereich des Gesetzes, zu dessen Vollzug er erlassen ist – so z.B. *Wolff/Bachof/Stober* 2000, § 48 IV, Rn. 48 – oder mit der Tatbestandswirkung des Verwaltungsakts im Bundesstaat begründet wird – so z.B. *Lerche* in: *Maunz/Dürig*, GG, Art. 83 Rn. 49f.

[795] S. den Regelungsvorschlag in Teil 3 Kap. 6.3 a.E.

[796] Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

[797] S. Teil 3 Kap. 3.1.

Die selbstgesetzten und anerkannten Verhaltensregeln werden von den verantwortlichen Stellen freiwillig akzeptiert. Um aber die notwendige Rechtssicherheit zu gewährleisten, sollte sich eine verantwortliche Stelle verbindlich erklären müssen, ob die Regeln für sie gelten sollen. Damit die betroffenen Personen wissen können, ob die Prinzipien für die betreffende Stelle gelten, sollte diese den Beitritt zu den Prinzipien sowie ihre Geschäftsbedingungen zum Datenschutz öffentlich bekannt machen.[798] Hat sie dies gegenüber der für sie zuständigen Kontrollstelle[799] erklärt, ist sie in ein öffentliches Register einzutragen, das von der Kontrollstelle geführt wird, die für den Sitz der Stelle zuständig ist.[800] Der BfD sollte die Listen zusammenführen und eine bundesweite Liste betreuen.

Im Entwurf für ein UGB war vorgeschlagen worden, rechtlich unverbindliche Selbstverpflichtungen in § 35 rechtlich näher zu strukturieren und die Überprüfbarkeit ihrer Einhaltung sicherzustellen.[801] Diese unverbindlichen Selbstverpflichtungen waren aber weder als normersetzend noch normkonkretisierend gedacht, sondern nur normvermeidend und nur für den Bereich der Umweltvorsorge vorgesehen. Hier sind freiwillige Verhaltensregeln aber als Konkretisierungen von Rechtsnormen vorgesehen und sollen auch in den Bereichen zur Anwendung kommen können, in denen die staatliche Schutzpflicht eingreift. Hierfür wären unverbindliche Verhaltensregelungen ungeeignet. Sie würden auch das Ziel einer Bindung der Kontrollstellen nicht erreichen. Insofern wird dem Vorbild des Entwurfs eines UGB in dieser Frage nicht gefolgt. Die hier vorgeschlagene Regelung schließt im Übrigen unverbindliche Selbstverpflichtungen von verantwortlichen Stellen nicht aus.

6.5.1 Verbindlichkeit der Verhaltensregeln

Welche Verbindlichkeit können die selbstgesetzten und anerkannten Verhaltensregeln haben? Sie sind kein allgemeinverbindliches Recht, da ihnen die notwendige über das Demokratieprinzip vermittelte personelle Legitimation fehlt. Ihre Verbindlichkeit ist daher adressatenbezogen differenziert zu beurteilen.

Für die *verantwortliche Stelle*, die die Verhaltensregeln für sich als verbindlich erklärt, gelten sie auf Grund dieser Selbstverpflichtung. Sie sollten für die verantwortliche Stelle solange verbindlich sein, wie die Anerkennung gilt.[802] Mit dieser Regelung wird – wie mit der vergleichbaren Regelung in § 3 Abs. 3 TVG für Tarifverträge – verhindert, dass die verantwortliche Stelle durch einfache Erklärung die Geltung der bisherigen Rechtsgrundlage für laufende Datenverarbeitungsprozesse einfach beseitigen kann. Damit wird das Vertrauen der betroffenen Personen geschützt. Soweit die Regelung des BDSG Drittschutz vermittelt, muss dies auch für deren Konkretisierung durch eine Verhaltensregel gelten.[803] Durch die Möglichkeit, durch selbstgesetzte Regeln die gesetzlichen Vorgaben zu konkretisieren, darf der Rechtsschutz der betroffenen Person nicht eingeschränkt werden.

---

798 Ebenso die Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 10; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 a) und Erwägungsgrund 7, EG-ABl. L 215 vom 25.8.2000, 7.

799 Da hier die für die verantwortliche Stelle geltende örtliche Zuständigkeit entscheidet, kann diese Kontrollstelle eine andere sein als diejenige, die die jeweilige Verhaltensregel anerkannt hat.

800 Ebenso die Safe Harbor Principles, nach denen die Federal Trade Commission ein öffentlich zugängliches Register führt, in dem alle den Grundsätzen beigetretenen Stellen aufgeführt sind – S. Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 10; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 a) und Erwägungsgrund 7, EG-ABl. L 215 vom 25.8.2000, 7.

801 S. hierzu näher UGB-KOM-E 1998, 507, 509.

802 S. zur vergleichbaren Regelung für öffentlich-rechtliche Verträge im Umweltrecht in § 36 Abs. 2 Satz 2 des Entwurfs eines UGB – s. zur Begründung auch UGB-KOM-E 1998, 511.

803 Eine vergleichbare Regelung sieht der Entwurf für ein UGB in § 36 Abs.4 vor – s. zur Begründung UGB-KOM-E 1998, 512.

Die Anerkennung der Verhaltensregeln durch die *Kontrollstelle*[804] ist ein feststellender Verwaltungsakt, der auch die feststellende Behörde bindet. Gesetzlich geregelt wird, dass auch alle anderen Kontrollstellen an die Feststellung der anerkennenden Kontrollstelle gebunden sind. Die Bindung gilt solange, wie der Verwaltungsakt Bestandskraft hat. Der Verwaltungsakt kann nach den allgemeinen Regeln zurückgenommen oder widerrufen werden. Solange dies nicht erfolgt ist, müssen die Kontrollstellen die Anerkennung bei ihrer Auslegung des Datenschutzrechts, bei ihrer Aufsichtstätigkeit und bei ihrem Handeln als Bußgeldbehörde beachten.

Für die *betroffenen Personen* haben die selbstgesetzten und anerkannten Regeln zwar insofern eine faktische Wirkung, als die Unternehmen sie ihrer Datenverarbeitung und die Kontrollstellen sie ihrer Aufsichtstätigkeit zu Grunde legen. Die Regeln sind für sie jedoch nicht rechtlich verbindlich. Sie können jederzeit die Rechtsauffassung geltend machen, dass die Verhaltensregeln den gesetzlichen Vorgaben widersprechen und eine ihnen folgende Datenverarbeitung rechtswidrig ist. Sie können ihre Rechtsauffassung in den in Kap. 6.5.3 genannten Schritten geltend machen.

Das Gleiche gilt für einen *Verbraucher- oder Datenschutzverband*, der einen Verstoß gegen Datenschutzrecht geltend macht. Selbst wenn er am Verfahren der Selbstregulierung beteiligt war,[805] kann er geltend machen, dass das Ergebnis die gesetzlichen Vorgaben nur unzureichend konkretisiert. Selbst in diesem Fall sind die selbstregulierten Normen allein Verhaltensregeln des normsetzenden Verbands. Auch wenn der Verband am Verfahren beteiligt war, ist ihm das Ergebnis der Selbstregulierung nicht zurechenbar. Etwas anderes kann allenfalls nach den Regeln des „venire contra factum proprium“ dann gelten, wenn er den Verhaltensregeln im Beteiligungsverfahren zugestimmt hat.

Eine betroffene Person kann die Datenverarbeitung, die auf den selbstregulierten Normen beruht, vor *Gericht* angreifen, indem sie vorträgt, dass diese Normen nicht den gesetzlichen Vorgaben entsprechen. Bei der Inzidenterprüfung dieser Frage ist das Gericht nicht an die selbstregulierten Normen gebunden. Es muss zwar die Anerkennung durch den feststellenden Verwaltungsakt der Kontrollstelle im Rahmen der Tatbestandswirkung des Verwaltungsakts anerkennen, ist aber an die Rechtsbewertung der Kontrollstelle nicht gebunden.

Dieses Ergebnis ist zwar hinsichtlich der Rechtssicherheit bezüglich der selbstgesetzten Normen nicht sehr befriedigend, angesichts der Rechtsschutzgarantie des Art. 19 Abs. 4 GG gegenüber jedem staatlichen Akt aber nicht zu vermeiden. Die Feststellung der Kontrollstelle, dass die Regeln der Selbstregulierung dem Datenschutzrecht entsprechen, muss gerichtlicher Überprüfung zugänglich sein. Ob dies große praktische Bedeutung hat, ist zu bezweifeln, da für das Handeln der verantwortlichen Stelle in erster Linie die Rechtsauffassung der Kontrollstelle entscheidend ist. Im Normalfall ist zu vermuten, dass auch die Gerichte sich dieser Rechtsauffassung anschließen werden.

6.5.2 Allgemeinverbindlichkeitserklärung von Verhaltensregeln?

Bei dem Fachgespräch mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde angeregt, die Verbindlichkeit der Verhaltensregeln dadurch zu erhöhen, dass sie für allgemeinverbindlich erklärt werden. Für eine solche Regelung könnte sprechen, dass sie Wettbewerbsverzerrungen ausgleichen würde: Verantwortliche Stellen, die anspruchsvolle – und eventuell über die gesetzlichen Anforderungen hinausgehende – Verhaltensregeln als für sich verbindlich anerkennen, müssen möglicherweise investieren, um diese Verhaltensregeln einhalten zu können. Sie könnten dadurch gegenüber Mitbewerbern Wettbewerbsnachteile erleiden oder befürchten und dadurch von der Anerkennung der

[804] S. hierzu Teil 3 Kap. 5.4.

[805] S. Teil 3 Kap. 6.3.

nachteile erleiden oder befürchten und dadurch von der Anerkennung der Verhaltensregeln abgehalten werden. Eine Allgemeinverbindlichkeitserklärung könnte für alle Mitbewerber gleiche Wettbewerbsbedingungen schaffen und dadurch die Umsetzung der Verhaltensregeln fördern.

Allgemeinverbindlichkeitserklärungen von Tarifverträgen[806] werden von § 5 TVG ermöglicht, um unerwünschte Arbeitsmarktentwicklungen bei rückläufiger Konjunktur verhindern zu können. Von rund 47.000 Tarifverträgen waren am 1.1.1998 rund 800 Tarifverträge allgemeinverbindlich.[807] Dabei geht es selten um Löhne und Gehälter, sondern überwiegend um gemeinsame Einrichtungen der Tarifvertragsparteien.[808]

Zuständig für die Allgemeinverbindlichkeitserklärung ist der Bundesminister für Arbeit, der den Tarifvertrag aber nicht verändern, die für alle verbindlichen Regelungen also inhaltlich nicht beeinflussen kann. Er kann auch nicht die Initiative ergreifen: Antragsberechtigt sind nur die Parteien, die den Tarifvertrag abgeschlossen haben. Weitere Voraussetzung ist, dass die Allgemeinverbindlichkeitserklärung im öffentlichen Interesse liegt. Außerdem darf die Erklärung nur erfolgen, wenn ausgeschlossen ist, dass eine Minderheit der Arbeitgeber die Mehrheit majorisiert. Daher müssen im Geltungsbereich des Tarifvertrags die tarifgebundenen Arbeitgeber mindestens 50 Prozent der unter den Tarifvertrag fallenden Arbeitnehmer beschäftigen. Schließlich setzt die Allgemeinverbindlichkeitserklärung das Einvernehmen mit dem Tarifausschuss voraus.[809] Dieser besteht aus je drei Vertretern der Spitzenorganisationen der Arbeitnehmer und Arbeitgeber, die der Minister auf Vorschläge der Spitzenorganisationen auswählt.[810] Mit der Ausgestaltung des Tarifvertrags, dem Antrag auf Allgemeinverbindlichkeitserklärung, der Majorität tarifgebundener Arbeitgeber und dem Tarifausschuss haben die Tarifparteien den weit überwiegenden Einfluss auf die für Außenseiter geltenden Zwangsregeln.

Nach dem Demokratieprinzip darf der Staat seine Bürger „nicht schrankenlos der normsetzenden Gewalt autonomer Gremien ausliefern ..., die ihm gegenüber nicht demokratisch bzw. mitgliedschaftlich legitimiert sind".[811] Hiervon macht aber Art. 9 Abs. 3 GG für die Aufgabe der Koalitionen, die Arbeits- und Wirtschaftsverhältnisse in Selbstverwaltung zu ordnen, eine Ausnahme. Sie dürfen Normen setzen, die Gesetze im materiellen Sinn sind.[812] Die Allgemeinverbindlichkeitserklärung ergänzt diese Normsetzungsprärogative der Tarifparteien im öffentlichen Interesse in den Fällen, in denen die Tarifparteien aufgrund der beschränkten Reichweite ihrer Regelung allein keine befriedigenden rechtlichen Regelungen erreichen können. Die Allgemeinverbindlichkeitserklärung ist somit ein Instrument, „das die von Art. 9 Abs. 3 GG intendierte autonome Ordnung des Arbeitslebens durch Koalitionen abstützen soll, indem sie den Normen der Tarifverträge zu größerer Durchsetzung verhilft".[813] Das Demokratiedefizit entspricht der Garantie des Kernbereichs der Koalitionsfreiheit und wird durch die

---

806 Das öffentliche Recht kennt z.B. auch die Allgemeinverbindlichkeitserklärung der von einem Beförderungsunternehmer festgelegten Beförderungsentgelte nach § 39 Abs. 1 Satz 2 PBefG. Dieses Beispiel erscheint aber für die hier anstehende Frage ein ungeeignetes Vorbild zu sein.

807 *Schaub*, Erfurter Kommentar, Rn. 4 – der BMA veröffentlicht regelmäßig Listen der allgemeinverbindlichen Tarifverträge. Nach *Däubler* 1993, Rn. 1245, betraf sie in der Weimarer Zeit rund 50% aller Tarifverträge.

808 *Däubler* 1993, Rn. 1246.

809 S. zu diesem § 1 DVO TVG.

810 *Schaub* 2000, Rn. 14.

811 *BVerfG*, AP 15 zu § 5 TVG, II 2 b) unter Verweis auf *BVerfGE* 33, 125 (158).

812 *BVerfG*, AP 15 zu § 5 TVG, II 1 b) aa).

813 *BVerfG*, AP 15 zu § 5 TVG, II 1 b) bb).

Voraussetzungen und das Verfahren der Allgemeinverbindlichkeitserklärung „hinreichend ausgeglichen".[814]

Das in § 5 TVG geregelte Verfahren ist auf die Selbstregulierung im Datenschutzrecht nicht übertragbar. Hiergegen sprechen neben dem unpassenden Verfahren vor allem, dass eine Allgemeinverbindlichkeitserklärung von Verhaltensregeln gegen das Demokratieprinzip verstoßen würde. Durch sie würden Regelungen eines nicht demokratisch legitimierten Gremiums ohne wesentlichen Einfluss demokratisch legitimierter Staatsorgane für Außenstehende für verbindlich erklärt, ohne dass dies von einer Ausnahmeregelung wie Art. 9 Abs. 3 GG ausgeglichen werden könnte. Außerdem ist der Zweck der Allgemeinverbindlichkeitserklärung im Tarifrecht nicht ohne weiteres auf das Datenschutzrecht übertragbar. Tarifverträge setzen an Stelle von Gesetzen Normen. Selbstgesetzte Verhaltensregeln im Datenschutz sind nicht gesetzesvertretend, sondern gesetzesausfüllend. Für diejenigen, für die sie nicht gelten, fehlen daher keine adäquaten Regelungen. Vielmehr gelten für diese die gesetzlichen Vorschriften. Es besteht somit ein viel geringeres Bedürfnis nach einer Allgemeinverbindlichkeitserklärung und damit auch eine erheblich geringere Rechtfertigung für einen solchen – eigentlich demokratiewidrigen – Akt.

Der Entwurf für ein UGB enthält in § 37 einen Vorschlag für eine Verbindlichkeitserklärung eines öffentlich-rechtlichen Vertrags, wenn diese im öffentlichen Interesse liegt und die Zahl der durch den Vertrag Verpflichteten nicht weniger als die Hälfte der durch die Verbindlichkeitserklärung Verpflichteten beträgt.[815] Die Verbindlichkeitserklärung soll allerdings durch eine normale Rechtsverordnung der Bundesregierung erfolgen, die sich den Inhalt des Vertrags zu eigen macht. Da der Vertrag nur über solche Gegenstände geschlossen werden darf, die nach § 13 des Entwurfs auch Inhalt einer Rechtsverordnung sein können,[816] könnte auch ohne die Vorschrift zur Verbindlichkeitserklärung eine Verordnung mit diesem Inhalt erlassen werden. Insofern erscheint diese Regelung überflüssig.[817] Sie vermag nicht als Vorbild für das Datenschutzrecht zu wirken.

Im Gegensatz zu den Konzeptionen im Tarifvertragsrecht oder im UGB, in denen den Verträgen eine normersetzende Funktion zukommt, haben die Verhaltensregeln hier „nur" eine gesetzesausfüllende Funktion. Ist für eine verantwortliche Stelle eine Verhaltensregel nicht verbindlich, fehlt nicht die einschlägige Regelung, sondern es kommt die gesetzliche Regelung unmittelbar zur Anwendung. In der hier vertretenen Konzeption ist ein „Auffangnetz" gespannt, das den Fall auffängt, dass die Selbstregulierung misslingt. Auch diese Konzeption zielt auf eine möglichst breite Erarbeitung, Anerkennung und Befolgung von Verhaltensregeln, ist aber vom Erfolg der Selbstregulierung nicht abhängig. Sie kann es sich daher leisten, auf das – zweifelhafte – Instrument einer Allgemeinverbindlichkeitserklärung – zumindest vorerst – zu verzichten.

6.5.3 Durchsetzung von Verhaltensregeln

Wenn die Verhaltensregeln verbindlich sein sollen, müssen sie auch wie gesetzliche Regelungen vollzogen und durchgesetzt werden. Ein Verstoß gegen diese selbst akzeptierten Regeln wird dann in der gleichen Form geahndet wie gegen gesetzliche Vorgaben. Dies ist mit dem

---

814 *BVerfG*, AP 15 zu § 5 TVG, II 2 b).

815 S. hierzu UGB-KOM-E 1998, 512f.

816 Ohne diese Regelung wäre die Verordnungsermächtigung zur Verbindlicherklärung zu unbestimmt und würde gegen Art. 80 GG verstoßen.

817 Im Datenschutzrecht fehlt die „Kultur" der Konkretisierung gesetzlicher Vorgaben durch Rechtsverordnungen und die hierfür erforderliche Vielfalt an Verordnungsermächtigungen. Insofern müsste hier auf eine gesetzliche Verbindlicherklärung Bezug genommen werden. Eine solche Regelung erscheint in noch stärkerem Maß überflüssig.

Demokratie- und Rechtsstaatsprinzip vereinbar. Da die selbstgesetzten Verhaltensregeln die gesetzlichen Regelungen nur konkretisieren, ist ein Verstoß gegen diese immer zugleich auch ein Verstoß gegen die gesetzlichen Verpflichtungen. Der Vollzug dieser Regeln unterscheidet sich daher nicht vom Vollzug gesetzlicher Regeln. Da die Straftat- und Ordnungswidrigkeitentatbestände ebenfalls auf die gesetzlichen Regelungen bezogen werden, können bei einer Verletzung von Verhaltensregelungen, die zugleich die gesetzlichen Pflichten betrifft, auch Strafen und Bußgelder verhängt werden. Anordnungen und Sanktionen dürften auf der Grundlage einer gesetzlichen Regelung kein Problem verursachen, soweit die selbstgesetzten Regeln zu einer Präzisierung der gesetzlichen Vorschriften führen. Denn die verantwortliche Stelle wird durch die selbstgesetzten Regeln nicht zusätzlich belastet, sondern allenfalls insoweit entlastet, als diese ihre Verpflichtung präzisieren.

Soweit die selbstgesetzten Regeln über die gesetzlichen Verpflichtungen hinausgehen, können sie eine Straftat oder eine Ordnungswidrigkeit nicht begründen. Diese können nur in dem Umfang bestehen, in dem gegen das gesetzlich geforderte Datenschutzniveau verstoßen wurde. Ein Verstoß allein gegen die weitergehenden Anforderungen selbstgesetzter Verhaltensregeln kann weder eine Strafe noch ein Bußgeld nach sich ziehen.

Für die Durchsetzung ist zu berücksichtigen, dass gerade im Bereich der Rechtsetzung durch Datenschutzklauseln in Allgemeinen Geschäftsbedingungen als einem Anwendungsgebiet der Selbstregulierung zahlreiche Rechtsverstöße festzustellen sind. Eine Selbstregulierung wird letztlich nur dann glaubwürdig und erfolgreich erfolgen können, wenn Verstößen durch ein präventiv wirkendes Haftungsrecht begegnet wird. Andererseits ist zu bedenken, dass kaum ein Unternehmen Verhaltensregeln für sich als verbindlich erklären wird, wenn damit eine Verschärfung seiner Haftungspflichten verbunden ist. Der mögliche Kompromiss zwischen präventiv wirkendem Haftungsrecht und Förderung der Selbstregulierung könnte darin bestehen, dass – wie bei den Straf- und Bußgeldregelungen – zwischen Verhaltensregeln zur Konkretisierung gesetzlicher Vorgaben und zusätzlichen, über diese hinausgehenden Verhaltensregeln unterschieden wird. Wenn das spezifische Datenschutzhaftungsrecht nur die gesetzlichen Anforderungen erfasst, gilt es nur für einen Verstoß gegen die gesetzlichen Normen. Soweit die Verhaltensregeln nur eine branchenspezifische Konkretisierung dieser Anforderungen betreffen, wird damit indirekt auch ein Verstoß gegen die selbstgesetzten Verhaltensregeln – allerdings als Gesetzesverstoß – erfasst. Damit führt das Unterwerfen unter gesetzeskonkretisierende Verhaltensregeln nicht zu einer haftungsrechtlichen Privilegierung,[818] die nicht zu begründen wäre, aber auch nicht zu einer Verschärfung der Haftungssituation. Vielmehr gilt weiterhin die allgemeine Haftung. Dagegen wird ein Verstoß allein gegen zusätzliche Verhaltensregeln von den spezifischen Datenschutzhaftungsregeln nicht erfasst. Dieser Kompromiss ist bei der Fassung der Haftungsregelungen zu berücksichtigen.[819]

Allerdings entspricht es dem Gedanken der wirtschaftlichen Selbstregulierung, wenn Verstöße gegen die selbstgesetzten Verhaltensregeln auch durch eine Unterlassungsklage durch Verbände und Vereine wie nach § 13 Abs. 2 AGBG und § 13 Abs. 2 UWG verfolgt werden können.[820] Dies wäre insbesondere für die selbstgesetzten Regeln klarzustellen. Auch über die gesetzlichen Anforderungen hinausgehende Verhaltensregeln können nicht öffentlich für ver-

[818] So auch vom Grundsatz her die Safe Harbor Principles – s. Grundsatz der Durchsetzung, Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 12; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 b) und Erwägungsgrund 5, EG-ABl. L 215 vom 25.8.2000, 7.

[819] S. Teil 3 Kap. 7.6.

[820] S. Teil 3 Kap. 9.3.

bindlich erklärt und danach ohne jede wettbewerbsrechtliche Sanktion ignoriert werden.[821] Das AGBG und das UWG kommen auf die gesamten Verhaltensregeln zur Anwendung und helfen dadurch auch die von Straf- und Ordnungswidrigkeitenregelungen sowie von den datenschutzspezifischen Haftungsregelungen nicht erfassten Teile der Verhaltensregeln durchzusetzen.

Die betroffene Person kann versuchen, ihre Interessen und Rechte auf vier Verfahrensstufen durchzusetzen:

- Beschwerde beim betrieblichen Datenschutzbeauftragten, der für Abhilfe sorgt[822] (Lösung auf Unternehmensebene),
- Beschwerde bei einer durch Selbstregulierung eingerichteten Schlichtungsstelle[823] (Lösung auf Verbandsebene),
- Beschwerde bei der Kontrollstelle, die die verantwortliche Stelle auf ihre Verpflichtungen hinweist – und nach einer Verweigerung der Abhilfe entsprechende Anordnungen trifft oder ein Bußgeld verhängt[824] (Lösung auf gesellschaftlicher Ebene),
- Klage vor Gericht (Lösung auf juristischer Ebene).

Die betroffene Person ist nicht verpflichtet, die vier Verfahrensstufen nacheinander zu beschreiten. Sie sind für sie voneinander unabhängige Angebote.

Für die ersten drei Verfahrensstufen wird das Gesetz durch anerkannte Verhaltensregeln verbindlich konkretisiert. Nur die Gerichte sind nicht an die Verhaltensregeln gebunden.[825]

Spezifische gesetzliche Regelungen sind für diese Verfahrensschritte nicht erforderlich, da sie sich aus anderen Regelungen implizit ergeben. Denkbar wäre allenfalls, dass für selbstregulierte Verhaltensregelungen ein Schlichtungsverfahren zum notwendigen Inhalt erklärt wird.

6.6 Wettbewerbsrechtliche Zulässigkeit

Datenschutzrechtliche Verhaltensregeln begründen neue Rahmenbedingungen für den Wettbewerb. Aus Wettbewerbsgründen kann es zur Umsetzung der Verhaltensregeln erforderlich sein, dass alle oder mindestens die wichtigsten Angehörigen des betroffenen Markts diese anwenden.[826] In solchen Situationen sichern die Unternehmen das von allen Mitbewerbern gewünschte Verhalten durch gegenseitige Verpflichtungserklärungen ab. Insofern tritt bei allen Formen der Selbstregulierung neben das vertikale Verhältnis zwischen Staat und Wirtschaftsunternehmen oder Wirtschaftsverband noch ein horizontales Verhältnis zwischen Wirtschaftsverband und seinen Mitgliedern oder zwischen den einzelnen Mitbewerbern am Markt selbst.[827]

Solche horizontalen Vereinbarungen können wettbewerbsbeschränkende Wirkung haben und sind daher grundsätzlich nach § 1 GWB unzulässig. Ob dies auch für staatlich initiierte Ab-

---

821 Auch nach den Safe Harbor Principles wird ein Verstoß gegen die freiwillig übernommenen Prinzipien als unlautere und irreführende Handlung sanktioniert – s. Grundsätze des „sicheren Hafens“ zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 10; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 b) und Erwägungsgrund 5, EG-ABl. L 215 vom 25.8.2000, 7.

822 S. Teil 3 Kap. 7.2.

823 S. Teil 3 Kap. 5.1 und 7.2.

824 S. Teil 3 Kap. 9.1.

825 S. Teil 3 Kap. 6.5.1.

826 S. für den Bereich des Umweltschutzes z.B. *Oldiges*, WiR 1973, 13f.; *Baudenbacher*, JZ 1988, 692.

827 S. z.B. *Oldiges*, WiR 1973, 10; *Baudenbacher*, JZ 1988, 691; *Brohm*, DÖV 1992, 1026; *Schmidt-Preuß*, VVDStRL 56 (1997), 215 Fn. 211.

sprachen zur Umsetzung von Allgemeininteressen gilt, ist umstritten. Überwiegend wird vertreten, dass das Kartellverbot nach § 1 GWB nicht zur Anwendung kommt, wenn der vom Staat inspirierte Inhalt der Abrede aufgrund einer speziellen gesetzlichen Ermächtigung in einem Gesetz festgelegt würde.[828] Das gleiche soll nach dieser Meinung auch bei staatlich inspirierten horizontalen Abreden gelten, die staatliche Regelungen der Wirtschaftslenkung ersetzen. Da staatliche wirtschaftslenkende Maßnahmen aus dem Kartellrecht ausgenommen sind, fallen nach dieser Meinung auch entsprechende Abreden zwischen den Unternehmen nicht unter das Kartellrecht. Über sie kann der Staat als Inspirator der Abrede kein Unrechtsurteil gemäß § 81 GWB aussprechen. Das Kartellrecht habe keine Kontrollfunktion gegenüber staatlicher Wirtschaftslenkung, sondern lediglich gegenüber privaten „wirtschaftslenkenden" Maßnahmen.[829] Allerdings fordert eine andere Meinung eine Genehmigung durch den Bundeswirtschaftsminister nach § 8 GWB.[830] Diese Vorschrift ermächtigt den Bundeswirtschaftsminister, die Erlaubnis zu einem wettbewerbsbeschränkenden Vertrag zu erteilen, wenn ausnahmsweise die Beschränkung des Wettbewerbs aus überwiegenden Gründen der Gesamtwirtschaft und des Gemeinwohls notwendig ist.

Zur Klarstellung, dass privatrechtliche Absprachen, die zur Umsetzung von Verhaltensregeln erforderlich sind, nicht am Wettbewerbsrecht scheitern, sollte das Gesetz eine sachbezogene Ausnahme vom Verbot wettbewerbsbeschränkender Verträge vorsehen. Diese Ausnahme ist davon abhängig zu machen, dass die Verträge oder Beschlüsse der Umsetzung von anerkannten Verhaltensregeln dienen, die Beschränkung des Wettbewerbs aus Gründen des Datenschutzes erforderlich ist und ein wesentlicher Wettbewerb auf dem Markt bestehen bleibt.[831]

Damit die beteiligten Behörden diese Voraussetzungen prüfen können, sind Verträge zwischen Unternehmen und Vereinigungen von Unternehmen sowie Beschlüsse von Vereinigungen von Unternehmen, die der Umsetzung von anerkannten Verhaltensregeln dienen, der zuständigen Kontrollstelle und der Kartellbehörde anzuzeigen. Die Kartellbehörde kann dann eventuell erforderliche Maßnahmen ergreifen. Sie wird zu den ersten beiden Voraussetzungen der Ausnahmeregelung sinnvoller Weise die Stellungnahme der zuständigen Kontrollstelle einholen.

Eine entsprechende Klarstellung könnte etwa folgendermaßen lauten:

(1) Verträge zwischen Unternehmen und Vereinigungen von Unternehmen sowie Beschlüsse von Vereinigungen von Unternehmen, die der Umsetzung von anerkannten Verhaltensregeln dienen, sind der zuständigen Kontrollstelle und der Kartellbehörde anzuzeigen.

(2) Auf Verträge und Beschlüsse nach Absatz 1 ist § 1 des Gesetzes gegen Wettbewerbsbeschränkungen nicht anwendbar, wenn

1. die Verträge oder Beschlüsse der Umsetzung von anerkannten Verhaltensregeln dienen,

2. die Beschränkung des Wettbewerbs aus Gründen des Datenschutzes erforderlich ist und

3. ein wesentlicher Wettbewerb auf dem Markt bestehen bleibt.

6.7 Evaluierung

Die Kontrollstellen sollen in ihren jährlichen Berichten auch immer über die Praxis der Selbstregulierung (Anerkennung, Selbstverpflichtungen, Durchführung, Vollzug) berichten, so dass diese unter einer ständigen Evaluierung steht.

---

828 S. z.B. *Kloepfer*, JZ 1980, 788; *Baudenbacher*, JZ 1988, 694; *Brohm*, DÖV 1992, 1027.

829 S. z.B. *Baudenbacher*, JZ 1988, 694f., *Brohm*, DÖV 1992, 1028; so wohl auch *Di Fabio* 1998, 131.

830 So aber z.B. *Kloepfer*, JZ 1980, 784 ff.; *Scherer*, DÖV 1991, 5; *Schmidt-Preuß*, VVDStRL 56 (1997), 216f.

831 S. hierzu auch einen vergleichbaren Vorschlag in § 39 des Entwurfs eines UGB – s. die Begründung in UGB-KOM-E 1998, 513 ff.

7. Rechte der betroffenen Personen

Informationelle Selbstbestimmung ist nur möglich, wenn die betroffenen Personen auch Mitwirkungsmöglichkeiten haben und die Datenverarbeitung beeinflussen können. Mitwirkungsmöglichkeiten setzen Transparenz über die Datenverarbeitung voraus. Daher sieht das deutsche Datenschutzrecht bereits umfassende individuelle Kontroll- und Mitwirkungsmöglichkeiten vor.[832]

An den Rechten der betroffenen Personen soll sich nichts Grundsätzliches ändern. Die Rechte auf Auskunft, Berichtigung, Widerspruch, Löschung, Sperrung und Schadensersatz sind den Entwicklungen anzupassen und um das Recht zum Selbstdatenschutz und zur Beschwerde, den Anspruch auf Anonymisierung und Pseudonymisierung der Daten und das Recht, die Kontrollinstanz einzuschalten, zu ergänzen.[833] Der dezentrale und weltweite Anfall der Daten, die technische und organisatorische Komplexität der Kommunikationsinfrastrukturen und wirtschaftlichen Abläufe, die Tatsache, dass Daten unsichtbar und unbemerkt erhoben werden können, sowie ihre zeitlich und quantitativ nahezu unbegrenzten Speicher- und Vervielfältigungsmöglichkeiten verringern die Transparenz drastisch, schließen einen Nachvollzug der Verarbeitungsvorgänge nahezu aus und führen zunehmend zu Kontrollverlusten der betroffenen Personen. Die so verschlechterten Verwirklichungsbedingungen der informationellen Selbstbestimmung müssen durch die Verstärkung der Betroffenenrechte und verfahrensrechtliche Vorkehrungen aufgefangen und ausgeglichen werden.

Betroffenenrechte bieten eine wesentliche Stütze für einen effektiven Datenschutz nur, wenn sie von den Betroffenen auch tatsächlich wahrgenommen werden.[834] Eine einfache Wahrnehmung der Rechte wird zur Zeit häufig dadurch behindert, dass die Betroffenen ihre Rechte schlicht nicht kennen, die Gesetze schwer verständlich formuliert und mit zahlreichen Ausnahmen versehen sind, sich die Anspruchsgrundlagen in unterschiedlichen Gesetzen befinden oder aber ihre Ausübung mit unangemessenem Arbeitsaufwand oder sogar Kosten verbunden ist.

Für eine zukünftige Regelung der Rechte der betroffenen Personen ergeben sich daher allgemeingültige Forderungen:

- Die betroffenen Personen müssen ihre Rechte frei und unbehindert ausüben können, ohne Zwang, dies zu tun oder nicht zu tun.
- Die Betroffenenrechte sollten, wenn möglich, nur im allgemeinen Datenschutzgesetz geregelt werden. Eine zusätzliche Normierung in bereichsspezifischen Regeln wäre eine unnötige Wiederholung, die nur zur Verwirrung auf Seiten der betroffenen Personen führt.[835] Eine Vereinheitlichung löst auch bestehende Wertungswidersprüche auf.[836]
- Betroffenenrechte sollten möglichst knapp und einfach formuliert werden, damit auch die Betroffenen selbst sie verstehen. Sie müssen ohne weiteres für jeden nachvollziehbar sein.
- Die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen ist auch bezüglich der Betroffenenrechte aufzugeben.

---

832 S. *Tinnefeld/Ehmann* 1998, 249 ff.

833 Ebenso *Simitis*, DuD 2000, 722.

834 Zweifelnd im Hinblick auf den tatsächlichen Informationsbedarf der Menschen allerdings *Bull*, RDV 1999, 150.

835 Sie müssten sich unter Umständen auf zwei oder mehr Auskunftsvorschriften berufen, auch wenn sie nur einen Datenverarbeiter ansprechen.

836 S. hierzu Teil 1 Kap. 2.4.2.

- Die Ausnahmetatbestände sollten auf ein notwendiges Minimum begrenzt werden. Bisher ist das Regel-Ausnahme-Verhältnis nahezu umgekehrt.
- Die Wahrnehmung der Betroffenenrechte sollte möglichst einfach sein. Aus diesem Grund sind insbesondere Medienbrüche zu vermeiden. Im Rahmen der Online-Kommunikation sollten die betroffenen Personen ihre Rechte daher auch telekommunikativ wahrnehmen können.[837]
- Die Betroffenenrechte müssen unentgeltlich wahrgenommen werden können.
- Die betroffene Person sollte bereits vor der Datenerhebung über ihre Rechte informiert werden. Die Informations- und Unterrichtungspflichten sind daher entsprechend auszuweiten.[838]
- Die Rechte der betroffenen Personen sind ausdrücklich für unabdingbar zu erklären. Sie dürfen nicht durch Rechtsgeschäft ausgeschlossen werden können.[839]

Die Stärkung der Rechte der betroffenen Person ist Teil des Konzepts zur Entlastung des Datenschutzrechts und der Datenschutzverwaltung.[840] Wenn die Parteien des Datenverarbeitungsverhältnisses rechtlich so ausgestattet sind, dass sie eigenverantwortlich und gleichberechtigt ihre Interessen wahrnehmen und ihre Konflikte austragen können, werden dadurch das Datenschutzrecht und die Datenschutzkontrolle von ihrer Schutzaufgabe entlastet: Die Konfliktregelung kann primär zwischen den Parteien stattfinden.

Wird die Ausübung der Rechte der betroffenen Person erleichtert, ist zu erwarten, dass sie auch häufiger erfolgt. Unter diesem Gesichtspunkt kommt den Betroffenenrechten, namentlich dem Auskunftsrecht, eine Funktion als „sanftes Druckmittel“ gegenüber den verantwortlichen Stellen zu. Eine häufige Nachfrage wird auch die verantwortlichen Stellen auf den Akzeptanzfaktor Datenschutz aufmerksam machen.

7.1 Auskunft

Das Auskunftsrecht ist die Grundlage aller weiteren Mitwirkungsrechte. Denn ohne die Möglichkeit zu erfahren, welche auf die betroffene Person bezogene Daten zu welchen Zwecken verarbeitet werden, kann diese gar nicht entscheiden, welche Mitwirkungsrechte sie ausüben möchte.[841] Daher stellte das Bundesverfassungsgericht fest:

> „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“[842]

Ebenso verlangt das Bundesverfassungsgericht im BND-Abhörurteil, dass der betroffenen Person Kenntnis über Erhebung und Speicherung gewährt wird, damit sie sich gegen unrechtmäßige Erfassungen und Weiterleitungen wehren kann.[843]

Das Auskunftsrecht ist ein Instrument vorgelagerten Rechtsschutzes.[844] Es gibt der betroffenen Person die Möglichkeit, die Verarbeitung ihrer Daten laufend zu kontrollieren. Daher sind

---

837 Hier kann eine Orientierung am TDDSG und MDStV erfolgen.

838 Beim Widerspruchsrecht jetzt vorgesehen, s. § 28 Abs. 4 Satz 2 BDSG.

839 Diese Einschränkung der Dispositionsbefugnis erfolgt im Interesse der betroffenen Person und ist bereits in § 6 BDSG vorgesehen.

840 S. hierzu Teil 2 Kap. 3.4.

841 S. z.B. *Mallmann*, GewArch. 2000, 354.

842 *BVerfGE* 65, 1 (43).

843 *BVerfGE* 100, 313 (361).

Eingriffe in das informationelle Selbstbestimmungsrecht durch einen Auskunftsanspruch abzumildern.[845] Das Auskunftsrecht ist für die betroffene Person das fundamentale individuelle Datenschutzrecht.[846] Es ergänzt die Transparenz, die durch individuelle Unterrichtung,[847] die Datenschutzerklärung[848] und durch die Veröffentlichung der Struktur und Funktionsweise der Datenverarbeitung[849] erzeugt wird.

7.1.1 Inhalt der Auskunft

Der Inhalt der Auskunft sollte sich – in Anlehnung an neue Landesdatenschutzgesetze – je nach Anforderung der betroffenen Person auf folgende Aspekte der Datenverarbeitung erstrecken:

- Gespeicherte Daten (auch Negativ-Auskünfte),
- Herkunft der Daten,
- Empfänger der Daten und Teilnehmer eines automatisierten Abrufverfahrens,
- Zweck der Datenverarbeitung,
- Auftragnehmer bei Datenverarbeitung im Auftrag und Dienstleister bei Funktionsübertragung,
- die erfolgte Berichtigung, Löschung oder Sperrung von Daten,
- Aufbau, Struktur und Ablauf der automatisierten Datenverarbeitung, insbesondere Profilbildungen und deren Struktur.

Soweit diese Informationen bereits in der Unterrichtung mitgeteilt oder in der Datenschutzerklärung veröffentlicht worden sind, entfällt der Auskunftsanspruch.

Das Auskunftsrecht muss sich allgemein – und nicht nur gemäß § 6a Abs. 3 BDSG – auch auf Aufbau, Struktur und Ablauf der automatisierten Datenverarbeitung beziehen. Nach Art. 12 a) DSRL muss nämlich auch „Auskunft über den logischen Aufbau der automatisierten Verarbeitung der betreffenden Daten“ gewährt werden. Sofern die verantwortliche Stelle diese Informationen bereits in ihrer Datenschutzerklärung veröffentlicht hat,[850] entfällt der Auskunftsanspruch, sofern keine Spezialfragen gestellt werden.[851] Unter dem Begriff „logischer Aufbau“ sind Angaben darüber zu verstehen, auf welche Informationen sich das System stützt und nach welchen Kriterien die Aufnahme und Strukturierung der Daten erfolgt.[852] Das Datenschutzrecht konzentriert sich damit nicht mehr nur auf den statisch gedachten Zustand der Speicherung und einzelne Transaktionen, sondern stellt den umfassend konzipierten Begriff der Verarbeitung ins Zentrum der Schutzüberlegungen.

---

844 *Bizer* 1992, 221.

845 *BVerfGE* 65, 1 (46); s. auch bereits *Steinmüller u.a.* 1971, 124.

846 Ein Auskunftsanspruch ist auch in Art. 8 der Datenschutzkonvention des Europarates von 1981 und in Nr. 13 der OECD-Leitlinien zum Datenschutz von 1980 enthalten.

847 S. Teil 3 Kap. 3.2.1 und 3.2.2.

848 S. Teil 3 Kap. 3.2.3.

849 S. Teil 3 Kap. 3.2.4.

850 S. Teils 3 Kap. 3.2.4.

851 Ein Auskunftsanspruch zu Strukturdaten fordert auch § 23 Abs. 1 Nr. 3 des Entwurfs eines BDSG von Bündnis90/Die Grünen.

852 *Schaar*, in: *Roßnagel*, RMD, § 7 TDDSG, Rn. 7. Der Erwägungsgrund 41 der Richtlinie enthält eine Präzisierung der europarechtlichen Vorgaben. Danach darf das Auskunftsrecht weder das Geschäftsgeheimnis noch das Recht am geistigen Eigentum berühren.

Auch Art. 11 Abs. 1 c) des portugiesischen Datenschutzgesetzes[853] fordert eine Auskunft über die „Logik" des Verarbeitungsprozesses. Section 26 (1) des finnischen Datenschutzgesetzes[854] fordert diese Auskunft nur bei der Datenverarbeitung für automatisierte Entscheidungen. Nach Section 7 (1 d) des britischen Data Protection Acts 1998[855] muss die Auskunft auch die „Logik der Entscheidungsfindung" umfassen, wenn eine automatische Verarbeitung von Daten zur Bewertung der Arbeitsleistung, der Kreditwürdigkeit, der Zuverlässigkeit, des Verhaltens oder ähnlicher Eigenschaften als einzige Grundlage für eine Entscheidung herangezogen wird. Dies gilt nach Section 8 (5) nicht, soweit diese „Logik" ein Geschäftsgeheimnis darstellt. Das italienische Datenschutzgesetz[856] gewährt in Art. 13 Abs. 1 c) 1) einen Anspruch auf Auskunft über Zweck und die Logik des Datenverarbeitungsprozesses.

Bei der Aufklärung der betroffenen Personen kommt es nicht unbedingt auf die Details an, sondern auf die tragenden Funktionsprinzipien der Anwendungsprogramme. Die betroffene Person muss verstehen können, in welcher Weise bestimmte Bewertungen und Klassifizierungen abgeleitet werden und welche Bedeutung diese Werte für ihr Persönlichkeitsrecht haben. Die Auskunft sollte daher Erläuterungen zur innerbetrieblichen Organisation, zum Ablauf des Verfahrens, zu den Kriterien, nach denen die Entscheidung erfolgt, und Angaben darüber, welche Gewichtung den einzelnen Bewertungskriterien gegeben wird, enthalten.[857] Insbesondere relevant dürfte dieser Inhalt der Auskunft zum Beispiel für Data-Warehouse- und Data-Mining-Verfahren, Scoring-Verfahren, Kundenkategorisierung und ähnliche Bewertungen betroffener Personen sein.

Die Auskunft muss sich – wie in § 7 TDDSG und § 16 MDStV – auch auf Pseudonyme erstrecken. Die betroffene Person muss Informationen über ihre Verwendung erhalten können. Da pseudonyme Daten verkettet und zu Profilen verarbeitet werden können, sollte die betroffene Person die Möglichkeit haben, Inhalt und Umfang der Datensammlung zu erfahren, um das Schadenspotential einer Aufdeckung ihres Pseudonyms abschätzen zu können.

7.1.2 Ausnahmen der Auskunftspflicht und Ausnahmenüberprüfungsverfahren

Für die Auskunftspflicht sind die zahlreichen Ausnahmen des geltenden Datenschutzrechts zu beschränken, da sie das Datenschutzrecht unnötig verkomplizieren.[858] Sie sind auch gemessen an den Vorgaben der Art. 12 und 13 DSRL zu weitgehend.

Die Ausnahmen sollten in Anlehnung an neuere Landesdatenschutzgesetze beschränkt werden

- für die Datenverarbeitung ohne gezielten Personenbezug sowie Kontroll- und Sicherungsdaten,[859]
- bei erheblicher Gefährdung eines zulässigen Verarbeitungszwecks,
- bei Gefährdung der öffentlichen Sicherheit oder eines Dritten,
- bei einer ausdrücklichen Geheimhaltungspflicht gegenüber der betroffenen Person.

---

853 Gesetz Nr. 67/98 zum Schutz personenbezogener Daten vom 26.10.1998.

854 Datenschutzgesetz (523/1999) vom 22.4.1999.

855 Data Protection Act vom 18.7.1998.

856 Gesetz Nr. 675 vom 31.12.1996.

857 Kritik bei *Koch*, MMR 1998, 461 mit Hinweis auf das Geschäftsgeheimnis der verantwortlichen Stellen.

858 Für öffentliche Stellen das Auskunftsrecht nach § 19 Abs. 1 BDSG mit den Ausnahmen in den Abs. 2 bis 5; für nicht-öffentliche Stellen das Auskunftsrecht nach § 34 Abs. 1 mit den Ausnahmen in Abs. 4 BDSG.

859 Ebenso z.B. § 18 Abs. 1 Satz 2 LDSG Nordrhein-Westfalen für Daten aus Datensicherungsmaßnahmen und der Datenschutzkontrolle.

Der Auskunftsanspruch zu einzelnen Daten sollte nur für die Datenverarbeitung mit gezieltem Personenbezug[860] gelten. Er sollte bei einer Datenverarbeitung ohne gezielten Personenbezug[861] entfallen, um nicht Data-Mining aus Gründen des Datenschutzes zu fordern.[862] Da bei dieser Form der Datenverarbeitung die Daten sofort gelöscht werden müssen, besteht auch kein praktischer Bedarf für das Auskunftsrecht. Es könnte sich nur auf die jeweils in der aktuellen Datenverarbeitung für die technische Leistungserbringung befindlichen Daten beziehen. Für diese Datenverarbeitung genügt die Veröffentlichung oder Auskunft über die Struktur der Datenverarbeitung.

Da einerseits eine Auskunft zu einzelnen Daten für den Datenschutz kontraproduktiv wäre und die informationelle Selbstbestimmung der betroffenen Person stärker beeinträchtigen würde und andererseits mit der Auskunft über die Struktur der Datenverarbeitung die für diesen Fall adäquate Transparenz für die betroffene Person geschaffen wird, kann das BDSG in Übereinstimmung mit Art. 13 Abs. 1 g) DSRL eine Ausnahme von der auf Einzeldaten gerichteten Auskunft vorsehen.[863]

Wenn die Daten der betroffenen Person gegenüber geheimgehalten werden müssen, sind die nicht geheimhaltungsbedürftigen Umstände mitzuteilen und die geheimhaltungsbedürftigen Umstände so zu umschreiben, dass die Auskunft so detailliert wie möglich ausfällt, ohne das Geheimnis zu verraten.[864] Dies gilt nicht, wenn bereits die Tatsache der Datenverarbeitung geheimgehalten werden muss.

Wenn von der verantwortlichen Stelle allgemein, nicht nur in einem Einzelfall Ausnahmen von der Auskunftspflicht geltend gemacht werden, sollte sie diese Ausnahmen an die Kontrollstelle melden müssen, damit diese prüfen kann, ob ein Ausnahmetatbestand generell vorliegt.

Bei einer Auskunftsverweigerung im Einzelfall kann die betroffene Person die Kontrollstelle anrufen und bei dieser beantragen, dass sie

- den Ausnahmetatbestand überprüft: Die verantwortliche Stelle muss ihr die Ausnahme plausibel machen und ihm notfalls sogar die geheim zu haltenden Daten zeigen. Bei nicht öffentlichen Stellen entscheidet die Kontrollstelle über die Berechtigung der Ausnahmen. Gegen diese Entscheidung ist der Rechtsweg zulässig.
- ersatzweise die Auskunft entgegen nimmt oder die Einsicht durchführt und die Rechtmäßigkeit der Datenverarbeitung prüft. Sie ist zur Wahrung des Geheimnisses verpflichtet und darf der betroffenen Person nur Auskünfte erteilen, die das Geheimnis wahren.

In anderen Bereichen des Rechts – etwa im Umweltrecht – sind Regelungen als zulässig anerkannt, die von dem zu Kontrollierenden fordern, der Kontrollstelle die Informationen preiszugeben, die diese für ihre Kontrollen benötigt, auch wenn es Geheimnisse sind. Die Kontrollstelle wird dadurch in den Kreis der Geheimnisträger aufgenommen. Der Schutz der Geheimnisse wird dadurch gewährleistet, dass die Kontrollstelle die ihr zugänglich gemachten Geheimnisse nicht an Dritte preisgeben darf.

---

860 S. Teil 3 Kap. 2.3.2.

861 S. Teil 3 Kap. 2.3.2.

862 S. hierzu auch Teil 3 Kap. 2.6.

863 Außerdem ist in §§ 19 Abs. 2, 34 Abs. 4 i.V.m 33 Abs. 2 Satz 1 Nr. 2 BDSG und in vielen Landesdatenschutzgesetzen die Auskunft über Daten aus der – insoweit vergleichbaren –Protokolldatenverarbeitung ausgeschlossen, ohne dass hierin ein Problem mit Art. 12 DSRL gesehen wird. Vielmehr wurde ausdrücklich auf Art. 13 Abs. 1 g) DSRL („Rechte und Freiheiten anderer Personen“) Bezug genommen – s. BT-Drs. 14/4329, 40.

864 S. hierzu auch die Vorschläge zur Regelung des Umgangs mit Geheimnissen in Teil 3 Kap. 3.2.4.

Das portugiesische Datenschutzgesetz[865] ermöglicht in Art. 11 Abs. 2, dass bei der Datenverarbeitung zum Zweck der Staatssicherheit, der Strafverfolgung und der Kriminalitätsvorbeugung das Auskunftsrecht stellvertretend von der Datenschutzkommission ausgeübt wird. Geht es um Gesundheitsdaten, kann das Auskunftsrecht nach Art. 11 Abs. 5 stellvertretend von einem Arzt ausgeübt werden, den die betroffene Person sich frei wählen kann.

7.1.3 Form und Verfahren der Auskunftserteilung

Die Auskunft soll unentgeltlich, unverzüglich[866] und vollständig erfolgen. Neben der schriftlichen Erteilung der Auskunft sollte auch eine elektronische Auskunft möglich sein. Diese kann auch elektronisch beantragt werden. Auskunftsfunktionen, die es dem Nutzer ermöglichen, einfach und schnell Anfragen an den Anbieter zu stellen und auf dem gleichen Wege unverzüglich Antwort zu erhalten, können die mit einem schriftlichen Ersuchen verbundenen faktischen Hindernisse für viele Betroffene beseitigen. Das Auskunftsrecht wird aufgewertet und erhält größere praktische Relevanz, die im Ergebnis auch zu einer Akzeptanzsteigerung bei den betroffenen Personen führen wird. So gesehen muss es auch im Interesse der verantwortlichen Stelle liegen, eine elektronische Auskunft zu ermöglichen.

Die Herausforderung liegt hier über die sinnvolle Integration in den geschäftlichen Kontext hinaus in der authentischen Absicherung eines Auskunftsbegehrens.[867] Denn es muss sichergestellt sein, dass nur die berechtigte Person Auskunft über personenbezogene Daten erhält. Die verantwortliche Stelle muss sich demnach vor der Erteilung der Auskunft über die Identität des Auskunftsersuchenden vergewissern. Das Verfahren und die Form der Identitätsprüfung bestimmt sie selbst.[868] Hier bietet sich die Nutzung elektronischer Signaturverfahren an.

Vielfach wird gefordert, dass das Auskunftsrecht auch die Möglichkeit der Einsichtnahme umfassen sollte. Die Umsetzung dieser Forderung setzt bei automatisierter Datenverarbeitung voraus, dass die verantwortlichen Stellen über einen Internetzugang verfügen, die Datenbanken und anderen Datenverarbeitungssysteme einen gesicherten und jeweils auf die Daten der betroffenen Person begrenzten Zugriff gewähren, die Daten in diesen personenbezogen gesammelt werden oder zusammengeführt werden können und diese über eine geeignete Oberfläche zur Darstellung der Daten verfügen. Sind die Daten der betroffenen Person mit Daten Dritter oder geheimhaltungsbedürftigen Daten verbunden, wäre vor der Einsichtnahme eine automatisierte Aufbereitung der Daten notwendig, die auskunftspflichtige Daten von den anderen Daten trennt. Schließlich müsste ein verlässliches automatisiertes Authentisierungsverfahren etabliert sein. Diese Voraussetzungen sind nur in den seltensten Fällen gegeben. Ein Recht auf Einsicht würde daher leerlaufen.

Eine automatisierte elektronische Einsicht sollte daher langfristig – in Form einer Zielfestlegung der Bundesregierung[869] – angestrebt werden, setzt derzeit aber noch weitere Entwicklungen und deren Förderung voraus. Bis dahin sollte ein Einsichtsrecht nur für die nicht automatisierte Datenverarbeitung vorgesehen werden. Sie wird nicht gewährt, soweit die personenbezogenen Daten mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Für die verantwortlichen Stellen sollte jedoch –

---

865 Gesetz Nr. 67/98 zum Schutz personenbezogener Daten vom 26.10.1998.

866 S. hierzu bereits § 7 TDDSG und § 16 MDStV.

867 S. hierzu z.B. das Forschungsprojekt „Datenschutz in Telediensten (DASIT)“, in dem eine Online-Einsicht im Rahmen einer prototypischen Realisierung eines Online-Shops mit Hilfe eines Java-Applets mit Betroffenenkontrollfunktionen ermöglicht wurde - s. zu DASIT näher z.B. *Grimm* 1999; *Grimm/Löhndorf/Roßnagel* 2000; *Enzmann*, DuD 2000, 535.

868 S. *Gola/Schomerus* 1997, § 34 Anm. 1.2.

869 S. zu diesem Instrument Teil 3 Kap. 6.2.

wie dies etwa § 27 Abs. 2 LDSG Schleswig-Holstein bereits vorsieht – in allen Verarbeitungsformen die Möglichkeit eröffnet werden, statt der Auskunft Einsicht in die zu der betroffenen Person gespeicherten Daten zu gewähren. Die Einsicht – wenn möglich online – zu ermöglichen, sollte als Zielsetzung formuliert werden, die die verantwortliche Stelle erreichen soll, soweit dies technisch möglich und verhältnismäßig ist.

Die Auskunftserteilung sollte bei einer automatisierten Datenverarbeitung, die immer auch über Suchfunktionen verfügt, nicht davon abhängig gemacht werden, dass die betroffene Person die Art der Daten, über die Auskunft verlangt wird, näher bezeichnet und zudem Angaben macht, die das Auffinden der Daten ermöglichen. Bei einer nicht automatisierten Datenverarbeitung kann die Suche nach bestimmten Daten sehr aufwändig sein. In diesem Fall können von der betroffenen Person Angaben gefordert werden, die das Auffinden der Daten ermöglichen. Die betroffene Person weiß jedoch unter Umständen nicht, ob die verantwortliche Stelle Daten über sie gespeichert hat. Sie muss zumindest die Möglichkeit haben, ihr Auskunftsbegehren in zwei Stufen zu präzisieren. In der ersten Stufe muss sie eine geeignete Übersicht über die von ihr gespeicherten Datenkategorien und die Verarbeitungsstrukturen erhalten, die ihr ermöglicht, in der zweiten Stufe ein konkretes Auskunftsbegehren zu formulieren.

Wird die Auskunft über pseudonyme Daten verlangt, muss das Auskunftsrecht unter Pseudonym geltend gemacht werden können, um durch die Geltendmachung des Anspruchs nicht das bisher genutzte Pseudonym zu verraten.[870] Der Diensteanbieter hat dem Träger des Pseudonyms unter seinem Pseudonym Auskunft über oder Einsicht in die Daten zu ermöglichen, die unter diesem Pseudonym gespeichert sind. Für die notwendige Authentisierung ist eine Aufdeckung des Pseudonyms jedenfalls nicht erforderlich. Vielmehr bieten sich auch ohne diese verschiedene zuverlässige Authentisierungsverfahren an. Am einfachsten und sichersten ist die Verwendung digitaler Pseudonyme, bei denen die Authentisierung über das Zertifikat möglich ist. Ist eine Authentisierung nicht möglich, kann zu einem Pseudonym keine Auskunft erteilt werden. Dies ist bei allen Pseudonymen unbefriedigend, die zwar verarbeitet werden, aber keine Authentisierung zulassen. Dennoch kann die Auskunft nur dem Träger des Pseudonyms und nur dann erteilt werden, wenn die auskunftsbegehrende Person nachgewiesen hat, zur Auskunft berechtigt zu sein.

Sollte die Auskunft auf Grund der zulässigen Ausnahmen verweigert werden, ist dies der betroffenen Person mitzuteilen. Sie ist darauf aufmerksam zu machen, ob sie eine Überprüfung der Entscheidung im Beschwerdeverfahren der verantwortlichen Stelle erreichen kann und welche Schritte sie hierfür zu unternehmen hat. Ansonsten ist sie darüber zu unterrichten, dass sie die Kontrollstelle einschalten kann, die an ihrer Stelle eine Auskunft erhalten muss.[871]

7.2 Beschwerde

Das Gesetz sollte – nach internationalem Vorbild – für alle verantwortlichen Stellen, die einen Datenschutzbeauftragten bestellen müssen, ein unentgeltliches Beschwerdeverfahren vorsehen. Jede betroffene Person kann den betrieblichen oder behördlichen Datenschutzbeauftragten als Beschwerdeinstanz anrufen. Er ist zur Prüfung der Beschwerde und zu ihrer Beantwortung verpflichtet. Er soll auf eine gütliche Lösung zwischen der verantwortlichen Stelle und der betroffenen Person hinwirken. Er muss innerhalb eines Monats eine schriftliche und mit Gründen versehene Antwort auf die Beschwerde abgeben.

Die Beschwerde ist ein für die betroffene Person einfacher Weg, einen Streit gütlich beizulegen, für sie aber nicht verpflichtend. Wenn sie diesen Weg beschritten hat, sollten aber bis zur

---

[870] S. hierzu *Schaar*, in: *Roßnagel*, RMD, § 7 TDDSG Rn. 37.

[871] S. Teil 3 Kap. 7.1.2.

Antwort des betrieblichen oder behördlichen Datenschutzbeauftragten die anderen Konfliktlösungswege verschlossen sein. Danach steht es der betroffenen Person wieder frei, die externe Kontrollstelle oder die Gerichte anzurufen. Fristen für Rechtsbehelfe werden während dieses Zeitraums gehemmt.

Sehen die Verhaltensregeln, der sich die verantwortliche Stelle unterworfen hat, ein – für die betroffene Person kostenloses, praktikables und effektives – Beschwerde- und Schlichtungsverfahren vor,[872] kann die Erhebung einer Klage von der unbefriedigenden Durchführung dieses Schlichtungsverfahrens abhängig gemacht werden.[873] Dies gilt nicht für Verfahren des einstweiligen Rechtsschutzes.

Die Beschwerdeinstanz und ihre Erreichbarkeit ist in der Datenschutzerklärung anzugeben. Alle Beschwerdeinstanzen bieten eine Hotline (Telefon und Email) an.[874]

Nach den Safe Harbor Principles müssen leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Beschwerdeverfahren geschaffen werden, nach denen der Beschwerde abgeholfen und auch – sofern dies das geltende Recht oder private Regelungen vorsehen[875] – Schadensersatz zugesprochen werden kann.[876] Im zukünftigen allgemeinen Datenschutzgesetz Japans wird ein „Dispute Resolution Procedure" für verantwortliche Stellen als verpflichtend vorgesehen. Als „Berufungsinstanz" kann für eine bestimmte Branche eine anerkannte Organisation der Datenverarbeiter vorgesehen werden.[877] Das Niederländische Datenschutzgesetz[878] sieht in Art. 25 Abs. 1 vor, dass die Datenschutzkommission selbstgesetzte Regeln, die eine eigene Streitschlichtung vorsehen, nur dann anerkennen darf, wenn sichergestellt ist, dass die Schiedsstelle unabhängig ist.

7.3 Widerspruchsrecht (Einwand)

Ein Recht zum Widerspruch wird von Art. 14 a) DSRL gefordert. Es bietet der betroffenen Person die Möglichkeit, gegen eine auf der Basis eines Erlaubnistatbestands an sich rechtmäßige Datenverarbeitung seinen abweichenden Willen geltend zu machen.[879] Soweit die Datenverarbeitung – wie vielfach im bisherigen Recht – nur erlaubt ist, wenn die verantwortliche Stelle keinen Grund zur Annahme hat, dass schutzwürdige Interessen der betroffenen Person überwiegen, ermöglicht der Widerspruch, solche überwiegenden Interessen bekannt zu machen, und damit im Regelfall die Realisierung einer Opt-out-Lösung.

Da in dem hier empfohlenen Konzept eine Opt-in-Lösung verfolgt wird und unbestimmte Abwägungsklauseln soweit möglich vermieden werden, wird die Bedeutung des Widerspruchs stark eingeschränkt, weil er überwiegend nicht erforderlich ist. Dennoch muss es der betroffenen Person immer möglich sein, ihren entgegenstehenden Willen geltend zu machen. Relevant wird der Widerspruch im Sinn einer Opt-out-Lösung, wenn der Datenverarbeiter die betroffene Person über die Erstellung eines Profils[880] oder über eine Funktionsübertragung[881]

---

872 S. Teil 3 Kap. 5.1.

873 S. hierzu das Beispiel des kanadischen Datenschutzgesetzes – s. *Huband*, DuD 2000, 461 ff.

874 S. Teil 3 Kap. 3.2.3.

875 Gegen diese Einschränkung sprach sich das *Europäische Parlament* aus, Resolution vom 5.7.2000, www.privacyinternational.org/issues/compliance/ep-safeharbor-700.html.; s. auch *Klug*, RDV 2000, 214.

876 S. den Grundsatz der Durchsetzung, Grundsätze des „sicheren Hafens" zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 12.

877 S. Japanische Expertenkommission 2000, 12.

878 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

879 S. hierzu z.B. *Simitis*, in: *ders. u.a.*, BDSG, § 28 Rn. 262; *Weichert*, WRP 1996, 522; *Breinlinger*, RDV 1997, 247; *Gola*, DuD 2001, 278; *Gola/Wronka*, RdA 1996, 217.

880 S. Teil 3 Kap. 3.5.4.

881 S. Teil 3 Kap. 3.5.6.

unterrichtet, wenn die verantwortliche Stelle annimmt, dass es sich um eine Datenverarbeitung handelt, die wegen der Offenkundigkeit der Daten oder der Art der Verarbeitung schutzwürdige Interessen der betroffenen Person offensichtlich nicht beeinträchtigen kann,[882] und die betroffene Person diese Einschätzung nicht teilt oder wenn die verantwortliche Stelle bereits vor Inkrafttreten der Novellierung rechtmäßig verarbeitete Daten weiter verarbeitet.[883]

Ansonsten kann die betroffene Person mit dem Widerspruch die besonderen Gründe geltend machen, die ihrer Meinung nach die konkrete Datenverarbeitung unzulässig machen. Ist der Widerspruch berechtigt, hat eine weitere Datenverarbeitung zu unterbleiben. Eventuell sind die Daten zu löschen oder zu sperren.

In Angrenzung zum Widerspruch nach § 69 VwGO sollte das Geltendmachen von Interessen, die einer Datenverarbeitung entgegenstehen, wie auch in § 29 Abs. 1 LDSG Schleswig-Holstein, „Einwand" genannt werden.

Das italienische Datenschutzgesetz[884] gewährt der betroffenen Person in Art. 13 Abs. 1 e) ein Widerspruchsrecht gegen die Datenverarbeitung zum Zweck der Marktforschung, der kommerziellen Kommunikation, der Werbung und des Marketing. Dies ist die konsequente Folge der Privilegierung dieser Datenverarbeitung in Art. 12 Abs. 1 f)[885] und der hierauf bezogenen Übermittlung und Verbreitung nach Art. 20 Abs. 1 e).[886] Ebenso sieht § 28 des Österreichischen Bundesgesetzes über den Schutz personenbezogener Daten[887] ein Widerspruchsrecht vor.

7.4 Berichtigung, Sperrung und Löschung

Die Rechte der betroffenen Personen auf Berichtigung, Sperrung und Löschung sollten beibehalten werden. Ergänzend zum geltenden Recht sollte die betroffene Person – nach dem Vorbild des Art. 13 Abs. 1 c) 4) des italienischen Datenschutzgesetzes[888] – einen Anspruch auf eine Bestätigung der verantwortlichen Stelle haben, dass diese die Berichtigung, Sperrung und Löschung bei sich durchgeführt sowie an die Empfänger der betroffenen Daten mitgeteilt hat. Dieser Anspruch soll dann nicht gelten, wenn seine Erfüllung unmöglich oder offensichtlich unverhältnismäßig ist. Das Österreichische Bundesgesetz über den Schutz personenbezogener Daten[889] setzt der verantwortlichen Stelle eine Frist von acht Wochen, um die Daten zu berichtigen, zu sperren oder zu löschen.

Diese Rechte können durch technische Mittel unterstützt werden. Mit Hilfe von Nutzerkontrollfunktionen[890] zur Inspektion, Löschung und Korrektur von personenbezogenen Daten und zum Erteilen und Widerrufen von Einwilligungen können diese Rechte über das Internet einfach ausgeübt werden.[891] Dieselben Funktionen können auch befugten Kontrolleuren zur Verfügung gestelllt werden

---

882 S. Teil 3 Kap. 2.2.

883 S. Teil 3 Kap. 10.

884 Gesetz Nr. 675 vom 31.12.1996.

885 S. hierzu Teil 3 Kap. 3.3.1.1.

886 S. Teil 3 Kap. 3.5.4.

887 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999.

888 Gesetz Nr. 675 vom 31.12.1996.

889 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999.

890 S. *Grimm* 1999.

891 Software zur Ausübung von Nutzerkontrollfunktionen wurde prototypisch im Forschungsprojekt DASIT entwickelt – s. z.B. *Grimm* 1999; *Grimm/Löhndorf/Roßnagel* 2000, 133; *Enzmann*, DuD 2000, 535; www.uni-kassel.de/fb10/oeff_recht/projekte/projekteDasit.ghk und www.sit.fraunhofer.de/MINT/index. html.

7.5 Anonymisierung und Pseudonymisierung

Ebenso wie die betroffene Person einen Anspruch auf Löschung hat, wenn die Datenverarbeitung für die Erfüllung des Zwecks nicht mehr erforderlich ist, sollte sie einen Anspruch geltend machen können, die Daten zu anonymisieren oder zu pseudonymisieren, wenn ihre Verfügbarkeit als identifizierbare Daten nicht mehr erforderlich ist. Dieser Anspruch kann in manchen Fällen zeitlich vor dem Anspruch auf Löschung liegen, in anderen Fällen wahlweise zu ihm geltend gemacht werden. Einen solchen Anspruch sieht beispielsweise auch Art. 13 Abs. 1 c) 2) des italienischen Datenschutzgesetzes[892] vor.

7.6 Schadensersatz

Der betroffenen Person muss ein Recht auf Schadensersatz zugestanden werden, wenn sie durch eine unzulässige oder unrichtige Verarbeitung personenbezogener Daten einen Schaden erleidet. Die allgemeinen Regelungen bieten hierfür keine ausreichende Rechtsgrundlage:

- Zwar besteht in vertraglichen oder vertragsähnlichen Beziehungen eine Anspruchsgrundlage nach den Grundsätzen der positiven Vertragsverletzung oder der culpa in contrahendo. Der sorgsame, gesetzeskonforme Umgang mit den personenbezogenen Daten des Vertragspartners dürfte regelmäßig auch eine Nebenpflicht der vertraglichen oder vertragsähnlichen Beziehung sein. Der Ersatz des Schadens ist allerdings auf Vermögensschäden begrenzt.[893]
- In Frage kommt auch ein Schadensersatzanspruch aus unerlaubter Handlung nach § 823 Abs. 1 BGB. Das allgemeine Persönlichkeitsrecht ist als „sonstiges Recht" im Sinn dieser Vorschrift und Datenschutzregelungen sind als Schutzgesetz im Rahmen des § 823 Abs. 2 BDSG anerkannt.[894] Außerdem kommt ein Schadensersatzanspruch nach § 824 BGB aus Kreditgefährdung,[895] nach § 826 BGB aus sittenwidriger Schädigung[896] und nach § 839 BGB aus Amtspflichtverletzung[897] in Frage. Ein Ausgleich immaterieller Schäden erfolgt in entsprechender Anwendung des § 847 BGB – allerdings nur dann, wenn die Verletzung des Persönlichkeitsrechts schwerwiegend ist und eine Genugtuung anders nicht angemessen gewährt werden kann.[898]

Im Datenschutzrecht sind in der Praxis bisher nur wenige Haftungsfälle bekannt geworden. Dennoch gelten die allgemeinen Haftungsregelungen für den Bereich der automatisierten Datenverarbeitung als unzureichend, weil für die Geschädigten der Nachweis sowohl der Ursächlichkeit als auch des Verschuldens nahezu unmöglich ist.[899] Daher sah der Gesetzgeber im BDSG 1990 für den öffentlichen Bereich eine Gefährdungshaftung und für den nicht öffentlichen Bereich eine Umkehr der Beweislast für Ursächlichkeit und Verschulden im Rahmen der genannten Anspruchsgrundlagen vor.[900]

---

892 Gesetz Nr. 675 vom 31.12.1996.

893 S. z.B. *Gola/Schomerus*, BDSG, § 8 Anm. 2.1.

894 S. z.B. *OLG Hamm*, MDR 1983, 667; *OLG Hamm*, NJW 1996, 131; *Bergmann/Mörle/Herb*, BDSG, § 8 Rn. 18; *Hamm*, ZIP 1983, 552; *Gola/Schomerus*, BDSG, § 1, Anm. 2.3; *Winkelmann*, MDR 1985, 718; Palandt-*Thomas*, § 823 BGB, Rn. 145.

895 S. z.B. *OLG Frankfurt*, RDV 1988, 148.

896 S. z.B. *Gola/Schomerus*, BDSG, § 8 Anm. 2.2.

897 S. z.B. *OLG Köln*, RDV 2000, 224.

898 Ständige Rechtsprechung seit dem Herrenreiter-Urteil, *BGHZ* 26, 349; s. z.B. *BGH*, RDV 1996, 132 – s. weitere Nachweise z.B. in *Gola/Schomerus*, BDSG, § 8 Anm. 3.

899 S. BR-Drs. 618/88, 108.

900 S. z.B. *Auernhammer*, BDSG, § 8 Rn. 3; *Gola/Schomerus*, BDSG, § 8 Anm. 1 und 4.

Das BDSG 2001 hat in Umsetzung von Art. 23 DSRL in dem neuen § 7 eine eigenständige Haftungsnorm für alle Formen der Datenverarbeitung aller verantwortlichen Stellen eingeführt, die entfällt, wenn die verantwortliche Stelle nachweist, dass sie die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.[901] Dadurch ist allerdings die Ursachenvermutung des BDSG 1990 entfallen. In § 8 wird die Gefährdungshaftung für die automatisierte Verarbeitung öffentlicher Stellen beibehalten. Nur ihnen gegenüber können Verletzungen des Persönlichkeitsrechts geltend gemacht werden.

Die Schadensersatzregelungen müssen neben der Ausgleichsfunktion vor allem auch einen spürbaren Anreiz für die korrekte Einhaltung der Datenschutzregelungen geben. Von der Haftungsregelung kann dann eine präventive Wirkung erwartet werden, wenn das Haftungsrisiko geringer wird oder gar entfällt, wenn die verantwortliche Stelle die datenschutzrechtlichen Pflichten nachweisbar vollständig erfüllt. Dadurch erhält insbesondere das Datenschutzmanagementsystem intern die bedeutungssteigernde Aufgabe, Haftungsrisiken und damit Versicherungsprämien zu vermindern.

Die datenschutzrechtlichen Schadensersatzregelungen dürfen andererseits nicht eine erwünschte Selbstregulierung verhindern.[902] Sie gelten daher nicht spezifisch für die selbstgesetzten Verhaltensregeln, sondern nur für die gesetzlichen Anforderungen. Soweit allerdings die Verhaltensregeln nur die gesetzlichen Anforderungen branchenspezifisch konkretisieren, ist ein Verstoß gegen die selbstgesetzten Verhaltensregeln zugleich ein Verstoß gegen die gesetzlichen Normen. Dagegen wird ein Verstoß allein gegen Verhaltensregeln, die über die gesetzlichen Mindestanforderungen hinausgehen, von den spezifischen Datenschutzhaftungsregeln nicht erfasst.

7.6.1 Einheitliche Gefährdungshaftung

Über die von § 7 BDSG umgesetzte Mindestregelung des Art. 23 DSRL hinausgehend sieht § 8 BDSG – wie auch alle neueren Landesdatenschutzgesetze – für die automatisierte Datenverarbeitung durch öffentliche Stellen eine Gefährdungshaftung vor. Grundlage der Gefährdungshaftung ist der Einsatz einer zwar erlaubten, aber gleichwohl gefährlichen Technik.[903] Die amtliche Begründung führt zur Gefährdungshaftung aus:

> „Angesichts der von der automatisierten Datenverarbeitung ausgehenden Gefahren für das Persönlichkeitsrecht[904] erscheint es angebracht, eine den Besonderheiten der modernen Datenverarbeitung angepasste Haftung vorzusehen. Die normale Verschuldenshaftung mit der uneingeschränkten Beweispflicht des Geschädigten wird diesen Besonderheiten nicht gerecht. Deshalb wird für bestimmte Tatbestände eine Gefährdungshaftung eingeführt. Diese trägt der vom BVerfG aufgezeigten besonderen Gefährdung des Persönlichkeitsrechts durch die automatisierte Datenverarbeitung dadurch Rechnung, dass sie das Risiko beim Einsatz dieser Technik, nämlich die technisch unbegrenzte Möglichkeit, auch falsche Daten dauerhaft speichern und in Sekundenschnelle ohne Rücksicht auf Entfernungen abrufen zu können, dem Betreiber auferlegt. In Anbetracht der komplexen, für außenstehende Dritte kaum nachvollziehbaren Vorgänge bei der automatisierten Datenverarbeitung kann es dem Betroffenen nicht zugemutet werden, dem Betreiber der Anlage ein Verschulden nachweisen zu müssen.“[905]

Diese Begründung entspricht den ansonsten überwiegend für Regelungen der Gefährdungshaftung geltend gemachten Gründen[906] – etwa für die Regelungen in § 7 StVG, § 33 LuftVG,

---

901 BT-Drs. 14/4329, 38.

902 S. hierzu Teil 3 Kap. 6.5.3.

903 S. z.B. *Müller/Wächter*, DuD 1989, 240.

904 *BVerfGE* 65, 1 (42).

905 BR-Drs. 618/88, 108.

906 S. z.B. *Müller/Wächter*, DuD 1989, 240.

§§ 1, 2 HPflG, §§ 25 ff. AtG, §§ 32 ff. GenTG. Eine andere Erwägung liegt jedoch der Regelung des § 22 WHG zugrunde. Diese Vorschrift knüpft die Gefährdungshaftung nicht an besonders risikoträchtige Tätigkeiten, sondern an das besondere Schutzbedürfnis des Umweltmediums Wasser. Für die datenschutzrechtliche Gefährdungshaftung kann auch diese Begründung herangezogen werden, da mit der bereits erfolgten und künftig verstärkt zu erwartenden nahezu explosionsartigen Zunahme der Verarbeitung personenbezogener Daten in gleichem Maß die besondere Schutzbedürftigkeit der informationellen Selbstbestimmung wächst.

Soll das bereits erreichte Haftungsniveau beibehalten und nicht vermindert werden, ist kein Grund ersichtlich,[907] die Gefährdungshaftung auf öffentliche Stellen zu begrenzen. Angesichts der gegenwärtigen und zukünftigen Risiken für die informationelle Selbstbestimmung, die von nicht öffentlichen Stellen zumindest in gleichem Maß ausgehen wie von öffentlichen Stellen,[908] erscheint eine Privilegierung privatwirtschaftlicher verantwortlicher Stellen nicht sachgerecht. Daher sollte sie für jede geschäftsmäßige automatisierte[909] Datenverarbeitung gelten.

Danach wäre folgende Differenzierung in der Haftung verantwortlicher Stellen vorzusehen: Die allgemeine Regelung des § 7 BDSG gilt zwar nominell für alle Formen der Datenverarbeitung, wird in der Praxis aber insbesondere für die nicht automatisierte und nicht geschäftsmäßige automatisierte Datenverarbeitung relevant. Dagegen wird sie für die geschäftsmäßige automatisierte Datenverarbeitung von der Gefährdungshaftung überlagert. Die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen wird aufgegeben. Diese Differenzierung ist am Risikopotenzial der Datenverarbeitung und nicht an der hierfür irrelevanten Organisationsform der verantwortlichen Stelle orientiert.

Um den Vollzug der Datenschutzregelungen zu unterstützen, sollte jedoch die Gefährdungshaftung entfallen und an ihre Stelle die allgemeine Haftungsregelung treten, wenn die verantwortliche Stelle nachweist, dass sie für den Zeitraum, in dem die Regelverletzung erfolgt sein kann, alle Anforderungen des Datenschutzmanagements erfüllt hat,[910] oder am Datenschutzaudit teilnimmt.[911] Mit einer solchen Entlastungsmöglichkeit durch Nachweis der Pflichterfüllung wird keine verdeckte Exkulpationsmöglichkeit eingeführt und die Gefährdungshaftung auch nicht zu einer verdeckten Verschuldenshaftung mit Beweislastumkehr. Vielmehr „belohnt" das Gesetz durch den Ausschluss der Gefährdungshaftung die Maßnahmen der verantwortlichen Stelle zur Verringerung des Risikos.[912] Weist die verantwortliche Stelle die Erfüllung aller technischen und organisatorischen Anforderungen an ihre Datenverarbeitung nach, geht von ihrer Datenverarbeitung keine gesteigerte Gefährdung für die informationelle Selbstbestimmung aus.[913] In diesem Fall erscheint es vertretbar, die besondere Risikoverteilung durch die Gefährdungshaftung aufzugeben und die allgemeinen Schadensersatzregeln für alle Formen der Datenverarbeitung zur Anwendung zu bringen.

---

907 Diese Unterscheidung wird auch in der amtlichen Begründung nicht begründet – s. BT-Drs. 14/4329, 38.

908 S. hierzu Teil 1 Kap. 2.1.

909 *Simitis*, in: *ders*. *u.a.*, BDSG, § 7 Rn. 8, kritisiert die Beschränkung auf die automatisierte Datenverarbeitung und fordert die Ausweitung der Gefährdungshaftung auch auf die manuelle Datenverarbeitung, ohne allerdings auf den Grund für die Gefährdungshaftung im Unterschied zur Verschuldenshaftung (besonders gefährliche Technik, „typische Automationsgefährdung" – s. BR-Drs. 618/88, 108; *Müller/Wächter*, DuD 1989, 239 – einzugehen.

910 Dieser Nachweis setzt eine umfassende und verlässliche Dokumentation voraus.

911 S. zu einer ähnlichen Entlastungsmöglichkeit – allerdings für eine vermutete Verschuldenshaftung – § 172 des Entwurfs für ein UGB sowie dessen Begründung in UGB-KOM-E 1998, 767 ff., 771f.

912 S. zur Forderung einer „Gefährdungshaftung mit Entlastungsmöglichkeit für Sorgfalt" im Umweltrecht z.B. *Ladeur*, VersR 1993, 263; *Godt* 1997, 161f.

913 Entlastung wegen „Verkehrsrichtigkeit" – s. *Godt* 1997, 161.

Für die Gefährdungshaftung ist eine Haftungshöchstgrenze vorzusehen[914] und für diese eine Deckungsvorsorge zu fordern. Die Haftungshöchstgrenze wird von § 8 Abs. 3 BDSG auf 250.000 DM pro Schadensfall unabhängig von der Zahl der Geschädigten festgelegt. Diese Regelung ist problematisch, wenn das gleiche Ereignis mehrere betroffene Personen schädigt.[915] Dagegen bestimmt zum Beispiel § 30 Abs. 3 LDSG Schleswig-Holstein, dass die gleiche Haftungshöchstgrenze pro Schadensereignis für jeden Geschädigten gilt. Diese Regelung entspricht sowohl dem Ausgleichs- als auch dem Steuerungszweck der Haftungsregelung besser und ist daher vorzuziehen.

Allerdings könnten sich durch die im Schadensfall ungewisse Haftungssumme Schwierigkeiten in der Versicherung dieses Haftungsrisikos ergeben. Sollte die Versicherungswirtschaft eine Versicherbarkeit ausschließen oder eine Versicherung wirtschaftlich nicht vertretbare Versicherungsprämien erfordern, müsste geprüft werden, bei welcher Gesamtschadensbegrenzung eine Deckungsvorsorge durch Versicherungen möglich erscheint. Diese dürfte jedenfalls bei einem Massenversicherungsmarkt deutlich höher liegen als bei 250.000 DM,[916] zumal die bisherige Praxis des Datenschutzhaftungsrechts zeigt, dass das Risiko eines Haftungsfalls relativ gering ist.[917] Außerdem entfällt die Gefährdungshaftung, wenn die verantwortliche Stelle nachweisen kann, alle Anforderungen des Datenschutzmanagements zu erfüllen, oder am Datenschutzaudit teilnimmt. Gegenüber dem Geschädigten wäre eine solche Haftungshöchstgrenze vertretbar, da er ja neben der Gefährdungshaftung immer auch die unbegrenzte Verschuldenshaftung geltend machen kann.

Um eine verdeckte Kommerzialisierung durch ein „Dulden und Liquidieren“ der betroffenen Person zu verhindern, sollte ein Schadensersatz ausscheiden, wenn die betroffene Person es schuldhaft unterlassen hat, den Schaden abzuwenden. Dies kann durch eine Anwendung des § 254 BGB erreicht werden.

Eine Gefährdungshaftung sehen auch Section 47 (1) des finnischen Datenschutzgesetzes[918] und Section 13 (1) des britischen Data Protection Acts 1998[919] vor. Dagegen übernahm zum Beispiel Section 48 des schwedischen Datenschutzgesetzes[920] den Wortlaut des Art. 23 DSRL.

7.6.2 Erleichterung des Kausalitätsnachweises

Nach allgemeinen Regeln müsste der Geschädigte, auch wenn er den Fehler der verantwortlichen Stelle und den Schaden nachgewiesen hat, den für ihn häufig sehr schwierigen oder unmöglichen Nachweis führen, dass der Schaden ursächliche Folge der unrichtigen oder unzulässigen Datenverarbeitung ist. Diese Schwierigkeit ist nicht in den Umständen des Einzelfalls begründet, sondern struktureller Natur. Zum Einen liegen die Schadensursachen in der Regel in einem Verfahren, dessen Organisation und Ablauf der betroffenen Person unzugäng-

---

914 Die Haftung nach § 31 Abs. 1 Satz 1 AtG und § 22 WHG ist allerdings unbegrenzt. Die anderen Regelungen zur Gefährdungshaftung enthalten dagegen eine Haftungsobergrenze, um eine Versicherung der Haftungsrisiken zu ermöglichen. Der Professoren-Entwurf für ein UGB sah keine Haftungsobergrenze für die Gefährdungshaftung vor, während der Entwurf für ein UGB durch die Unabhängige Kommission in § 184 eine Haftungsobergrenze empfahl.

915 S. z.B. *Gola/Schomerus*, BDSG, § 7 Anm. 2.3; *Simitis*, in: *ders. u.a.*, BDSG, § 7 Rn. 28.

916 Im Vergleich dazu beträgt die gesetzliche Haftungshöchstgrenze für ein Kraftfahrzeug nach § 12 StVG 850.000 DM.

917 Nach *Gola/Schomerus*, BDSG, § 7 Anm. 2.3 ist noch kein einziger Fall der Gefährdungshaftung für öffentliche Stellen bekannt geworden. Nach *Simitis*, in: *ders. u. a.*, BDSG, § 7 Rn. 27 sind es nur „recht seltene Schadensfälle“.

918 Datenschutzgesetz (523/1999) vom 22.4.1999.

919 Data Protection Act vom 18.7.1998.

920 Datenschutzgesetz (1998:204) vom 29.4.1998.

lich und intransparent ist. Zum Anderen sind zumeist nicht das Vermögen selbst, sondern „nur“ Arbeits- und Vermögenschancen betroffen.[921] Dass die Nichteinstellung eines Bewerbers, die Nichtgewährung eines Kredits oder der Ausschluss von einer Ausschreibung auf eine unzulässige Datenverarbeitung zurückzuführen ist, ist oft offensichtlich, aber zugleich nicht vollständig beweisbar.[922]

Hier sollte das Gesetz – wie von 1990 bis 2001 in § 8 BDSG und entsprechend dem Vorbild des Umwelthaftungsrechts[923] – eine Beweiserleichterung bieten: Wenn die betroffene Person die Rechtswidrigkeit oder Unrichtigkeit der Datenverarbeitung sowie Umstände des Einzelfalls belegt, die eine ganz überwiegende hohe Wahrscheinlichkeit für die Ursächlichkeit des entstandenen Schaden begründen, soll die verantwortliche Stelle nachweisen müssen, dass ihr Fehler den Schaden nicht verursacht haben kann. Diese Beweismaßreduzierung trägt den Besonderheiten durch Datenverarbeitung verursachter Schäden Rechnung, bei denen eine vollständige Überzeugung hinsichtlich des Vorliegens der haftungsbegründenden Kausalität im Sinn des § 286 Abs. 1 ZPO typischerweise nicht erreicht werden kann. Die Vermutung kann zu einer behutsamen Fortentwicklung des Beweisrechts durch die Rechtsprechung beitragen. Andererseits bleibt das Beweismaß so hoch, dass die verantwortliche Stelle nicht mit einer Verdachtshaftung belastet wird.[924] Die Ursachenvermutung wird regelmäßig dann nicht eingreifen, wenn die verantwortliche Stelle nachweist, dass sie alle Anforderungen an ihr Datenschutzmanagement erfüllt hat.[925] Der Nachweis kann auch durch die erfolgreiche Teilnahme am Datenschutzaudit erfolgen. Eine solche kompromisshafte Regelung entlastet nicht nur den Geschädigten von einem ihm oft unmöglichen Nachweis und verteilt die Beweislasten gerechter nach Einfluss- und Risikobereichen, sondern steigert auch das Interesse der verantwortlichen Stelle an einer Einhaltung der datenschutzrechtlichen Vorgaben und deren Dokumentation.

7.6.3 Umfang des Schadensersatzes

Neben materiellen Schäden sollten auch gewichtige immaterielle Schäden anerkannt werden.[926] Sie sind bei einer Verarbeitung personenbezogener Daten das eigentliche Risiko. Um zu verhindern, dass jede – auch kleinste – Belastung der betroffenen Person durch eine Verletzung von Datenschutzrecht (Beispiel: Ärger über unvollständige Unterrichtung) zu Schadensersatz führt, sollte der Anspruch – in Übereinstimmung mit der Zivilrechtsprechung zu Persönlichkeitsrechtverletzungen[927] – bei immateriellen Schäden auf schwere Verletzungen des Persönlichkeitsrechts beschränkt werden, wie dies in § 8 Abs. 2 BDSG und in fast allen Landesdatenschutzgesetzen vorgesehen ist.[928] Diese Regelung sollte für jede Form der Datenverarbeitung gelten, nicht nur wie bisher für die Gefährdungshaftung öffentlicher Stellen.

Auch der britische Data Protection Act 1998[929] sieht in Section 13 (2) einen Schadensersatz für „distress“ vor, wenn der Geschädigte auch einen materiellen Schaden erlitten hat oder die Regelverletzung, die Grund für den immateriellen Schaden ist, durch eine Datenverarbeitung für journalistische, künstlerische oder literarische Zwecke erfolgt ist.

---

921 Zu deren Ausgleich s. das folgende Kapitel.

922 S. *Weichert*, NJW 2001, 1466.

923 S. § 6 UmwHaftG und § 176 des Entwurfs eines UGB.

924 S. hierzu UGB-KOM-E 1998, 774; Professoren-Entwurf 1990, 428.

925 Dies wird ihr vor allem dann leicht fallen, wenn sie an einem Datenschutzaudit teilnimmt.

926 Eine Unterscheidung zwischen materiellen und immateriellen Schäden wird von Art. 23 DSRL nicht getroffen – s. z.B. *Dammann/Simitis*, Art. 23 Rn. 5; *Brühann/Zerdick* CR 1996, 435; *Lütkemeier*, DuD 1995, 600.

927 S. z.B. *BGHZ* 26, 347; 39, 124; 73, 120; *BGH*, RDV 1994, 245; *BGH*, RDV 1996, 132; *BAG*, DB 1985, 2307.

928 S. zu dieser Einschränkung kritisch *Simitis*, in: *ders. u.a.*, BDSG, § 7 Rn. 8, 23.

929 Data Protection Act vom 18.7.1998.

Die hier erörterte spezifische Schadensersatzregelung könnte etwa folgendermaßen lauten:

(1) Fügt eine verantwortliche Stelle einer natürlichen betroffenen Person durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung ihrer personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger zum Ersatz des Schadens verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. In schweren Fällen kann die geschädigte Person auch wegen eines Schadens, der kein Vermögensschaden ist, eine angemessene Entschädigung in Geld verlangen. Die §§ 254 und 852 des Bürgerlichen Gesetzbuches finden Anwendung.

(2) Ist der Schaden nach Absatz 1 durch eine geschäftsmäßige automatisierte Datenverarbeitung entstanden, besteht die Ersatzpflicht unabhängig von einem Verschulden der verantwortlichen Stelle. In diesem Fall haftet der Ersatzpflichtige gegenüber jeder geschädigten Person für jedes schädigende Ereignis bis zu einem Betrag von X Euro und für alle betroffenen Personen zusammen für jedes schädigende Ereignis bis zu einem Betrag von X Euro. Die Haftung nach Satz 1 entfällt, wenn die verantwortliche Stelle nachweist, dass sie für den Zeitraum, in dem der Schaden verursacht worden sein kann, die Anforderungen an das Datenschutzmanagement (§§ X - Y) erfüllt oder erfolgreich am Datenschutzaudit teilgenommen hat.

(3) Die Verursachung eines Schadens wird vermutet, wenn nach den Umständen des Einzelfalles eine ganz überwiegende Wahrscheinlichkeit besteht, dass der Schaden durch die unzulässige oder unrichtige Verarbeitung der verantwortlichen Stelle verursacht worden ist.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen verarbeitungsberechtigt und ist der Geschädigte nicht in der Lage, die verarbeitende Stelle festzustellen, so haftet jede dieser Stellen.

7.7 Bereicherungsausgleich

Eine Regelung, die einen Bereicherungsausgleich ermöglicht, wie sie in den Fachgesprächen zum Gutachten mehrfach gefordert wurde, scheint nicht erforderlich zu sein. Wenn bei der verantwortlichen Stelle durch eine rechtswidrige Datenverarbeitung eine Bereicherung eingetreten ist, kann die betroffene Person diese nach § 812 BGB im Weg der Eingriffskondiktion heraus verlangen.[930] Eine Verfügung oder Vermögensverschiebung, wie sie § 816 BGB fordert, ist für die Eingriffskondiktion nach § 812 BGB nicht erforderlich. Die Bereicherung besteht in der Ersparnis von Aufwendungen, die für eine berechtigte Verwertung der Daten zu zahlen gewesen wäre.[931]

7.8 Recht zum Selbstdatenschutz

Die Verwendung von Mitteln des Selbstdatenschutzes[932] dient der Gewährleistung des Grundrechts auf informationelle Selbstbestimmung. Sie darf außer in gesetzlich begründeten Fällen der betroffenen Person nicht verwehrt werden. Die Nutzung der Selbstschutzmittel darf nicht zur Diskriminierung der betroffenen Person führen. Ein Spezialfall dieses Rechts, ist das bereits erörterte Recht, den Personenbezug der eigenen Datenspuren auszuschließen, indem die betroffene Person anonym oder pseudonym handelt.[933] Dieses speziellere und das hier angesprochene allgemeine Recht der betroffenen Person sind zusammenzufassen.

---

930 S. für den vergleichbaren Fall der schuldlosen Verletzung eines Gebrauchsmusters oder Patents *BGH*, NJW 1977, 1194.

931 S. hierzu *Weichert*, NJW 2001, 1466.

932 S. Teil 2 Kap. 2.2.

933 S. Teil 3 Kap. 5.1.

7.9 Recht zur Anrufung der Kontrollstelle

Die bereits in § 21 BDSG gewährleistete Möglichkeit, sich an den Bundesbeauftragten für den Datenschutz wenden zu können, wenn die betroffene Person der Ansicht ist, durch die Datenverarbeitung öffentlicher Stellen in ihren Rechten verletzt worden zu sein, sollte auf den nicht öffentlichen Bereich ausgedehnt werden. Jede Person sollte die Möglichkeit haben, jede Kontrollstelle hinsichtlich der Datenverarbeitung durch jede verantwortliche Stelle anrufen zu können.

8. Technik und Organisation der Datenverarbeitung

Datenschutz wird in Zukunft nur möglich sein, wenn versucht wird, die technische Entwicklung in der Weise zu beeinflussen, dass Datenschutzaspekte von Anfang an berücksichtigt werden oder sogar als Ziel die Entwicklung der Informations- und Kommunikationstechnik anleiten. Hierfür bedarf es geeigneter Rahmenbedingungen, die in ihrer rechtlichen Form in diesem Gutachten angesprochen wurden, aber auch weit darüber hinausgehender staatlicher Unterstützung und Förderung.

8.1 Datenschutzfördernde Technik

Dies betrifft in erster Linie die Entwicklung und Einführung datenschutzfördernder Techniken (Privacy Enhancing Technologies) und „datensparsamer“ Verfahrensgestaltung, die die Gefahren für die informationelle Selbstbestimmung reduzieren können.[934] Im Sinn von Selbstorganisation und Selbstdatenschutz sind hierzu hinreichende Anreize zu schaffen.[935]

Alle Maßnahmen, die Anonymität oder Pseudonymität umsetzen, sowie diejenigen Phasen des Verarbeitungsprozesses, in denen personenbezogene oder -beziehbare Daten verarbeitet werden, müssen, soweit möglich, für die betroffenen Personen genauestens nachvollziehbar sein (Transparenz). Zu diesem Zweck sind wo immer möglich Komponenten und Systeme einzusetzen, deren Entwurf und Produktion lückenlos dokumentiert und öffentlich ist. Es ist als eine Aufgabe staatlicher Wirtschaftsförderung anzusehen, die Entwicklung und das Angebot solcher Systeme zu fördern.[936]

Wünschenswert wäre in diesem Zusammenhang die Einrichtung einer Institution, wie etwa eines Forschungsinstituts der Datenschutzbeauftragten des Bundes und der Länder, das damit beauftragt wird, den aktuellen Stand der Risiken für die informationelle Selbstbestimmung ebenso wie den Stand der Schutztechniken fortlaufend zu beobachten und aufzubereiten. Es würde den Stand der Technik dadurch beeinflussen und damit das rechtliche Gebotene voranbringen, indem es diese Kenntnisse veröffentlicht, Entwickler und Anwender berät und beispielhafte Realisierungen anstößt.

8.2 Querschittsregelungen zur Verwendung bestimmter Techniken

Für die Gestaltung und die Verwendung bestimmter Techniken sind spezifische Querschnittsregelungen zu empfehlen.

8.2.1 Audio-visuelle Systeme

Die in § 6b BDSG nach langem politischen Ringen gefundene Regelung sollte vorerst nicht neu entschieden werden. Gleichwohl muss darauf aufmerksam gemacht werden, dass die bisherige phänotypisch klare Abgrenzung, was Videoüberwachung ist, von neuen Techniken herausgefordert werden wird: Bei UMTS werden massenhaft Terminals mobil eingesetzt werden, die zur Videoüberwachung geeignet sind: Mobiltelefone werden mit einer Videoka-

[934] S. Teil 3 Kap. 4.3.1.
[935] S. Teil 3 Kap. 4.3.2.
[936] S. Teil 3 Kap. 4.3.3.

mera ausgestattet sein, mit der der Besitzer des Mobiltelefons jederzeit auf Sendung gehen kann – sei es nach Hause, hin zur Stammkneipe,[937] zu einer Videoüberwachungszentrale, zur nächsten Polizeidienststelle oder auch zu einer Fernsehstation.[938] Inwieweit der Gesetzgeber künftig solche Nutzungsformen der Übertragungstechnik regeln soll, bedarf eingehender Diskussion.[939] Jedenfalls ist die Sensor- und Übertragungstechnik zu einer umfassenden, jederzeitigen und allgegenwärtigen audio-visuellen Überwachung *geeignet*. Für UMTS gilt dies mit Abstrichen, für Nachfolgetechnologien uneingeschränkt.

Möglichkeiten, die Videokamera und das Mikrofon eines Terminals vom Netz aus einzuschalten – ganz gleich ob dies eine vom Hersteller unbewusst oder gar bewusst eingebaute Sicherheitslücke ist oder ob dies auf Betreiben sogenannter Bedarfsträger offiziell eingebaut wurde – würden UMTS und Nachfolgetechnologien zu einer nie dagewesenen, für Massenüberwachung geeigneten Technologie machen. Es sei hier noch einmal an die zuvor beschriebenen Transparenzforderungen an jede Informations- und Kommunikationstechnik erinnert, die mit personenbezogenen Daten in Berührung kommen kann.

8.2.2 Mobile Datenverarbeitung

Die gegenwärtigen Regelungen zur mobilen Datenverarbeitung in der Definition des § 3 Abs. 10 BDSG und in den Anforderungen des § 6c BDSG adressieren ein reales und künftig stark zunehmendes Problem: Personen werden dadurch beobachtbar, dass sie kleine Geräte mit sich führen, die von der Umgebung sehr leicht verfolgt werden können – oder dies gar routinemäßig werden. Solche kleinen Geräte können *kontaktbehaftete Chipkarten* sein, die immer verfolgt werden können, wenn sie in ein Lesegerät gesteckt werden – etwa beim Arzt oder beim Händler zur Bezahlung. *Kontaktlose Chipkarten* steigern dieses Datenschutzproblem, indem sie nicht nur gelesen werden können, wenn der Besitzer einen bewussten Akt wie das Einführen in ein Lesegerät vornimmt, sondern immer dann, wenn der Besitzer sie bei sich führt und in die Nähe einer Lesestation kommt. Für manche Anwendungen ist dies verlockend bequem, wie beispielsweise beim Einsteigen in öffentliche Verkehrsmittel, wo das Ein- und Aussteigen automatisch registriert und dem Kunden der Komfort einer Bestabrechnung angeboten werden kann – dem misstrauischen Lebenspartner beispielsweise aber auch rückwirkend ein Bewegungsprofil zur Überprüfung vermeintlicher Ausreden.

Sogenannte RFTAG – kleinste Spulen, die wenn sie mit einem Hochfrequenzsignal angeregt werden, eine sie identifizierende eindeutige Kennung zurücksenden – werden künftig für wenige Cent produzierbar und so klein sein (deutlich kleiner und leichter als ein Konfetti), dass sie in viele Gegenstände des täglichen Gebrauchs integriert sein werden. Diese Anwendung wird ganz harmlos damit beginnen, dass im Supermarkt alle Produkte statt mit Preisaufklebern mit RFTAG versehen werden. Dann braucht man den Einkaufswagen nur noch an einer Lesestation vorbeizuschieben, die alle RFTAG anregt und deren Kennungen registriert und auswertet. Schon kann eine Einkaufsliste ausgedruckt und der Gesamtbetrag des Einkaufs kassiert werden. Die gleiche Technik der Preisauszeichnung wird auch bei Kleidung angewendet werden – und schon tragen alle leicht verfolgbare Personenkennzeichen mit sich herum. Wer dies wann und in welcher Situation nutzt, ist beim (Ver-)Kauf beispielsweise eines Kleidungsstücks nicht vorhersehbar. Dies gilt umso mehr, sollte solch ein Kleidungsstück mit auf Auslandsreisen genommen werden, wo das deutsche Recht keinen direkten Einfluss auf die dort betriebenen Informations- und Kommunikationssysteme hat.

---

[937] Schon eine kurze Life-Übertragung aus einer Peep-Show kann ganz erheblich in die Rechte der Darstellerin oder des Darstellers eingreifen.

[938] Dies macht ganz neue Sendungen unter dem Schlagwort „Die aktuelle Kamera“ möglich.

[939] Die gilt vor allem, wenn die in Teil 3 Kap. 4.3.1 genannten Anforderungen an Entwicklung und Herstellung diese Risiken nicht zu reduzieren vermögen.

Sowohl die Definition der mobilen Datenverarbeitung als auch die Anforderungen an diese müssen dieser Entwicklung angepasst werden. Eventuell müssen sogar neue Regelungen und Begriffe eingeführt werden, da nach der jetzigen Regelung beispielsweise RFTAG und vergleichbare Techniken nicht erfasst werden. Abzustellen ist dabei nicht nur auf den intendierten Gebrauch, sondern auch auf den möglichen Missbrauch.

Für die künftige Definition der mobilen Datenverarbeitung ist zum Beispiel zu berücksichtigen, dass

- Gegenstände wie RFTAG nicht ausgegeben werden, sondern in andere Gegenstände, wie in einem gekauften Produkt, integriert sind,
- eine Speicherung und erst recht eine Verarbeitung personenbezogener Daten auf dem mobilen Medium für die Gefährdung der informationellen Selbstbestimmung nicht nötig ist und beispielsweise auf RFTAG auch nicht stattfindet,
- es bei RFTAG keinen Gebrauch des Mediums gibt, der vom Betroffenen beeinflusst werden könnte; bei kontaktlosen Chipkarten gibt es ihn nahezu nicht.

Für die Formulierung von Schutzanforderungen ist daher zu berücksichtigen, dass

- es keine verantwortliche Stelle gibt, die sowohl das Medium ausgibt oder verkauft und alle Anwendungen verantwortet. RFTAG sind universell verwendbar – isoliert für sich betrachtet aber vollkommen harmlos und ohne jede Datenverarbeitung.
- das Auskunftsrecht nicht auf das mobile Medium beschränkt werden darf, sondern sich auf alle involvierten Informations- und Kommunikationssysteme erstrecken muss,
- für die geforderte Transparenz nicht nur auf Kommunikationsvorgänge abgestellt werden darf, die auf dem mobilen Medium eine Datenverarbeitung auslösen, sondern auf alle Vorgänge abgestellt werden muss, die in irgendeiner Form eine Datenverarbeitung auslösen, in die das Medium einbezogen ist – egal wo sie abläuft.

8.2.3 Biometrische Verfahren

Bei biometrischen Verfahren sind zwei Aspekte zu unterscheiden: die Sicherheit und mögliche Nebenwirkungen. *Sicherheit* bedeutet, dass die richtige Person akzeptiert wird, falsche Personen aber abgewiesen werden. Dies sind die Primärziele von Biometrie im Kontext von Sicherheit der Informations- und Kommunikationstechnik. *Mögliche Nebenwirkungen* sind, dass

- bei nahezu allen biometrischen Verfahren medizinische Informationen oder andere für das Verhalten der Person relevante Informationen erfasst werden. Die Möglichkeit sie auszuwerten besteht immer – unabhängig davon, ob dies tatsächlich geschieht. Die daraus folgenden Befürchtungen biometrischer Verhaltensauswertung sind daher nicht von der Hand zu weisen. Dies hat Auswirkungen auf die soziale Kommunikation, indem betroffene Personen in der Wahrnehmung ihrer Rechte eingeschränkt werden oder unfreiwillig ihr Verhalten den Gefahren anpassen.
- bei vielen Verfahren eine Art Personenkennzeichen entsteht, da voraussichtlich nur relativ wenige biometrische Merkmale in der Praxis verwendet werden und jedes verwendbare Merkmal bezogen auf eine Person vergleichsweise stabil und dauerhaft sein muss.

Während verantwortliche Stellen ein primäres Interesse an dem Aspekt der biometrischen Sicherheit haben, muss das Datenschutzrecht die darüber hinausgehenden Risiken berücksichtigen und entsprechende Forderungen erheben:

- Biometrische Verfahren sind so auszuwählen und so zu gestalten, dass bei ihnen so wenig medizinisch relevante Informationen wie möglich erfasst werden können.

- Die erfasste Information ist so früh wie möglich so zu sogenannten Templates zu verdichten, dass in den Templates nachweislich keine medizinisch oder für das Verhalten relevante Information mehr enthalten ist.
- Damit biometrische Merkmale nicht als Personenkennzeichen dienen können, sind vorzugsweise solche biometrischen Verfahren einzusetzen, bei denen der Betroffene durch eine bewusste Handlungsvariation für unterschiedliche erfasste Informationen und statistisch unkorrelierte Templates sorgen kann. (Dieses bewusste Verhalten ist auch unter den Aspekten Transparenz und Steuerbarkeit (=Willenserklärung) durch den Betroffenen von Vorteil.)
- Da Menschen ihre biometrischen Eigenschaften nicht ändern können, nur weil sich die Informations- und Kommunikationstechnik in dem Sinn als unsicher herausgestellt hat, dass die primär erfassten Merkmale oder Templates von Personen kompromittiert wurden, so dass sie nun unabhängig von der Person genutzt werden können, müssen alle biometrischen Systeme vor ihrem Ersteinsatz bezüglich der Erfüllung dieser Forderungen geprüft und zertifiziert werden.

8.2.4 Automatisierte Einzelentscheidungen

Die in § 6a BDSG gefundene Regelung zu automatisierten Einzelentscheidungen ist eine erste – und soweit dieses Gebiet bisher verstanden ist – bis auf eine Formulierungsungenauigkeit gelungene Umsetzung der Vorgabe von Art. 15 der DSRL. Um Missverständnissen vorzubeugen und die Regelungsziele der Bestimmung noch effektiver zur Geltung zu bringen, sollte sie indes präzisiert und ergänzt werden.

Die aktuelle Formulierung des § 6a Abs. 1 „... dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen." ist insoweit missverständlich, als die automatisierten Einzelentscheidungen auch auf Eingabedaten beruhen können, die für sich betrachtet nicht der Bewertung einzelner Persönlichkeitsmerkmale dienen. Die Gefahr geht weniger von den verwendeten Daten aus, als vielmehr von der automatisierten Verarbeitung selbst, deren Ergebnisse zu Beeinträchtigungen der Betroffenen führen können. Erst durch die Verarbeitung „dienen" die Daten der Bewertung von Persönlichkeitsmerkmalen. Ein Beispiel ist die Ableitung der Kreditwürdigkeit aus dem Wohnort, der für sich genommen nicht der Bewertung einzelner Persönlichkeitsmerkmale dient. Die englischsprachige Formulierung der Richtlinie „... which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him" lässt offen, ob sich „intended to evaluate certain personal aspects" auf das „processing" oder auf „data" bezieht. Auch beschränkt sich die englische Formulierung nicht auf „einzelne" Persönlichkeitsmerkmale. Aus den dargestellten Gründen wird eine modifizierte Formulierung vorgeschlagen:

„Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Datenverarbeitung gestützt werden, die der Bewertung von Persönlichkeitsmerkmalen des Betroffenen dient."

Ausgangspunkt für eine grundsätzlichere Betrachtung sind aus technischer Sicht zwei Regelungsziele:

1. Es soll sichergestellt werden, dass die als Entscheidungsgrundlage genommene Information richtig, aktuell, vollständig und relevant ist.
2. Die Entscheidungsfunktion ist richtig – man könnte auch sagen „angemessen" – und wird korrekt und nachvollziehbar ausgeführt. Dies ist der Kern der automatisierten Einzelentscheidung.

Beide Regelungsziele können allein mit technischen Mitteln, die derzeit zur Verfügung stehen, nicht umfassend sichergestellt werden:

1. Zwar kann innerhalb eines technischen Systems weitgehend sichergestellt werden, dass Informationen unverändert und in der im technischen System jeweils aktuellen Version sowie in den im technischen System bekannten Zusammenhängen auch vollständig dargestellt werden. Der Aspekt der Relevanz wie auch der Aktualität in Bezug auf die reale Welt entzieht sich jedoch weitgehend dem, was technische Systeme jetzt und in der überschaubaren Zukunft zu leisten in der Lage sind.
2. Zwar kann bei einfachen Entscheidungsfunktionen (z.B.: Ist das Jahreseinkommen, vermindert um 10000 DM pro unterhaltsberechtigter Person größer als 40000 DM?) ein IT-System weitaus zuverlässiger, weil ermüdungsfreier, als ein Mensch entscheiden, allerdings stellt sich bei komplizierten Entscheidungsfunktionen immer sowohl die Frage ihrer Richtigkeit und Angemessenheit wie auch ihrer richtigen Umsetzung.

§ 6a BDSG unterscheidet nicht zwischen 1. Informationsbereitstellung und 2. Entscheidung. Möchte man eine detailliertere Regelung, dürfte diese Unterscheidung sowie eine nähere Bestimmung der „Relevanz" von Daten für eine Entscheidung aus technischer Sicht die wesentliche nächste Detaillierungsstufe sein. Der in § 6a gewählte Ansatz, die technischen Sachverhalte nicht genauer zu unterscheiden und folglich auch nicht genauer zu regeln, sondern stattdessen an den Interessen des Betroffenen anzuknüpfen (Abs. 2 Nr. 1.) oder an seiner Möglichkeit, seinen Standpunkt geltend zu machen, ist aus technischer Sicht zur Zeit angemessen.

Die technischen Grenzen berücksichtigend sollten für eine künftige Regelung zu automatisierten Einzelentscheidungen die Betroffenenrechte erweitert und entsprechend in Erwägung gezogen werden, dass die Geltendmachung ihres Standpunktes durch die betroffene Person nach § 6a Abs. 2 Nr. 2 Satz 2 BDSG nicht nur zu einer Revision der ursprünglich für ihn negativen Entscheidung führt, sondern auch zu einer Revision der über ihn gespeicherten Informationen sowie der ihn betreffenden Entscheidungsfunktion. Nur so kann verhindert werden, dass die betroffene Person sich immer wieder gegen eine für sie nachteilige Entscheidungsfunktion wehren muss.

9. Datenschutzkontrolle

Die Kontrolle des Datenschutzrechts ist eine unabdingbare Voraussetzung für die Verwirklichung des Ziels, das Recht auf informationelle Selbstbestimmung auch in einer informatisierten Gesellschaft angemessen schützen zu können. Das Bundesverfassungsgericht hat hierzu bereits 1983 festgestellt:

> „Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen automatischer Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung."[940]

Die Aufgabe der Kontrolle ist eine wichtige, aber nicht die einzige Aufgabe der Datenschutzbeauftragten. Sie ist auch nicht allein ihre Aufgabe. Sie wären damit überfordert. Um auch nur ansatzweise eine effektive Kontrolle zu erreichen, die das vom Bundesverfassungsgericht formulierte Ziel einer Sicherung der informationellen Selbstbestimmung erreichen kann, ist eine Ergänzung der staatlichen Fremdkontrolle (Kap. 9.1) durch eine Selbstkontrolle in Form betrieblicher und behördlicher Datenschutzbeauftragter (Kap. 9.2) und eine gesellschaftliche

[940] *BVerfGE* 65, 1 (46).

Kontrolle durch die betroffenen Personen, vor allem aber Vereinigungen und Verbände, die sich im Datenschutz engagieren (Kap. 9.3), erforderlich.

9.1 Staatliche Kontrollstellen

Das deutsche Datenschutzrecht ist ein föderatives Rechtsgebiet. Die Gesetzgebungskompetenz liegt im öffentlichen Bereich sowohl beim Bund als auch bei den Ländern, im nicht öffentlichen Bereich beim Bund. Die öffentliche Kontrolle nehmen arbeitsteilig der Bund und die Länder wahr. Diese föderative Ausrichtung hat die Entwicklung des Datenschutzes nachhaltig befruchtet. Es war mit Hessen ein Bundesland, das die Vorreiterrolle übernahm und bereits sieben Jahre vor dem Bund ein Landesdatenschutzgesetz verabschiedete. Diese föderative Ausrichtung sollte auch in Zukunft beibehalten werden.

Gleichwohl ist es für einen effektiven Datenschutz in der Bundesrepublik und für eine Vereinfachung des Datenschutzrechts unabdingbar, dass sich die Datenschutzstandards auch in Zukunft auf einem gleich hohen Niveau bewegen. Diesem Ziel tragen die inoffiziellen Gremien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für den öffentlichen Bereich und der Düsseldorfer Kreis für den nicht öffentlichen Bereich schon heute Rechnung.

Wenn im Folgenden die Rolle und die Aufgaben der öffentlichen Kontrollstellen allgemein angesprochen werden, so beziehen sich die Forderungen und Anregungen häufig sowohl auf die Bundes- als auch auf die Landesebene. Den Gutachtern ist bewusst, dass sich der originäre Einfluss des Bundesgesetzgebers nur auf die Ausgestaltung des Amtes des Bundesbeauftragten und die inhaltliche Ausrichtung der Kontrolle im nicht öffentlichen Bereich beziehen kann. Daher verstehen sie ihre Anregungen auch als Appell an die Landesgesetzgeber. Eine enge inhaltliche Abstimmung zwischen Bund und Ländern wird auch in Zukunft wichtig sein.

Die Organisationsform der Kontrollstellen, ihre Stellung in der Staatsorganisation und ihre Unabhängigkeit sind kein Selbstzweck, sondern wirken sich unmittelbar auf die Wirksamkeit der Datenschutzkontrolle, auf die Kooperationswilligkeit der zu Kontrollierenden und auf die gesellschaftliche und persönliche Akzeptanz des Datenschutzes und seiner Hüter aus.

9.1.1 Einheitliche Kontrollstellen

Die unterschiedlichen Zuständigkeiten für die Aufsicht über datenverarbeitende Stellen in Deutschland einschließlich der Sonderzuständigkeiten im Bereich der Telekommunikation, bei Mediendiensten und Rundfunkanstalten müssen vereinfacht werden. In erheblichem Rahmen kann dies erreicht werden, wenn die Länder – wie in einigen Fällen bereits geschehen – die für den nicht öffentlichen Bereich zuständigen Aufsichtsbehörden funktional den Landesbeauftragten für den Datenschutz übertragen.[941]

Eine funktionale Zusammenlegung der datenschutzrechtlichen Aufsicht ist bereits aus europarechtlichen Erwägungen geboten.[942] Die Aufspaltung der Datenschutzkontrolle in einen öffentlichen und einen nicht öffentlichen Sektor ist der europäischen Richtlinie (Art. 28) sowohl hinsichtlich der Organisationsform als auch hinsichtlich der Befugnisse fremd.

Die Einführung der Initiativkontrolle auch im privaten Bereich stellt einen intensiveren Eingriff des Staats in die Unternehmenssphäre als bisher dar. Aus diesem Grunde sollten die Kontrollstellen im privaten Bereich in möglichst weiter Ferne zu anderen Bereichen der Exekutive mit ihren spezifischen Interessen angesiedelt sein. Die bereits bestehenden unabhängigen Datenschutzbehörden bieten sich dafür an.

---

941 Mit unterschiedlichen Begründungen *Bäumler*, DuD 2000, 21; *Bizer*, DuD 1997, 482; *Garstka*, DuD 2000, 290; *Simitis*, NJW 1997, 287.

942 S. *Dammann/Simitis*, Einl. Rn. 44.

Zudem lässt sich die Einbindung der Aufsichtsbehörden in die Ministerialbürokratie, wie sie bisher überwiegend praktiziert wird, und die daraus folgende Weisungsgebundenheit auch aus Gründen der von der DSRL geforderten „völligen Unabhängigkeit" der Kontrollstellen[943] nicht länger rechtfertigen.[944] Die Institutionalisierung von weiteren völlig unabhängigen Stellen neben den öffentlichen Datenschutzbeauftragten – dies wäre die Konsequenz einer Perpetuierung der zweigeteilten Datenschutzkontrolle – würde weitaus größere Schwierigkeiten für den Verwaltungsaufbau mit sich bringen, als eine Zusammenführung der Aufgaben unter einem Dach.

Eine Vereinheitlichung der Kontrollstellen entspricht den Prinzipien der Verwaltungsmodernisierung, die sich an Effizienz, Bündelung und Qualitätsmanagement orientiert.[945] Sie ist angesichts der Gleichartigkeit der Aufgaben im öffentlichen und nicht öffentlichen Bereich auch aus Akzeptanz- und fiskalischen Gründen geboten:

- Dem Einzelnen erleichtert es die Wahrnehmung seiner Rechte im Datenschutz, wenn er sich an ein und dieselbe Instanz wenden kann. Im Bewusstsein der durchschnittlich informierten Öffentlichkeit gibt es Bundes- und Landesdatenschutzbeauftragte, die für die Einhaltung des Datenschutzes zuständig und Ansprechpartner Hilfe suchender Bürger sind. Nur wenigen ist die Zuständigkeit unterschiedlicher Behörden in einem Land bekannt. Es ist nur schwer zu vermitteln, dass gerade im nicht öffentlichen Bereich – der angesichts der zunehmenden Verarbeitung personenbezogener Daten immer mehr als Bedrohung für die Privatsphäre empfunden wird –, nicht der unabhängige öffentliche Datenschutzbeauftragte zuständig ist, sondern ein Ministerium oder Regierungspräsidium, bei dem diese Aufgabe als untergeordnete, bestenfalls mit vielen anderen Aufgaben gleichgeordnete Aufgabe verstanden wird.
- Dualismus führt zur Verschwendung von Ressourcen und durch unterschiedliche Auslegungs- und Verwaltungspraktiken zur Herausbildung verschiedener Verfahrensweisen in der Datenschutzkontrolle, mithin zu einem unterschiedlichen Datenschutzniveau.
- Die Konzentration beider Kontrollbereiche entlastet die Ministerialverwaltung von ministerialfremden Aufgaben.
- Ohnehin führt die zunehmende Auslagerung von vormals öffentlichen Dienstleistungen in den privaten Sektor dazu, dass die verschiedenen Kontrollräume nur noch schwer zu trennen sind.

Sowohl bei der Beratung der Vorfassungen zu diesem Gutachten in der Begleitkommission[946] als auch im Schrifttum[947] wurde vor einer Zusammenführung der Datenschutzkontrolle im öffentlichen und nicht öffentlichen Bereich gewarnt. Zum einen wurde geltend gemacht, die Zweiteilung beruhe auf einer sinnvollen funktionalen Differenzierung der Verwaltungskompetenzen im Datenschutz. Zum anderen wurde befürchtet, dass durch die mit der Kontrolle über den nicht öffentlichen Bereich verbundene Befugnisserweiterung die Unabhängigkeit der Datenschutzbeauftragten gefährdet wäre. Dies wird insbesondere dadurch erwartet, dass diese administrative Akte erlassen, die zu einer gerichtlichen Nachprüfung führen können. Die auf Vertrauen beruhende Beratungsfunktion des Datenschutzbeauftragten würde durch gerichtliche Auseinandersetzungen verdrängt, der Einfluss und das politische Gewicht, das gerade auf

943 S. Teil 3 Kap. 9.1.2.

944 *Simitis*, NJW 1997, 287.

945 *Bäumler*, DuD 2000, 21.

946 S. die Zusammenfassung der zweiten Sitzung der Begleitkommission am 25.6.2001 in Anhang 3.2, S. 250.

947 *Kloepfer* 1998, D 133, D 148.

seiner Beschränkung auf öffentliche Kritik beruht und aus sich heraus bereits effektvoll ist, entwertet.

Zum ersten Gegenargument ist festzustellen, dass für den öffentlichen und den nicht öffentlichen Bereich nach dem hier vorgeschlagenen Konzept weitgehend die gleichen materiellen Anforderungen an die Datenverarbeitung gestellt werden. Damit entfällt auch der innere Grund für die funktionale Differenzierung.

Das zweite Gegenargument betrifft nicht unmittelbar die funktionale Trennung, sondern in erster Linie die Befugnis der Kontrollstellen im nicht öffentlichen Bereich. Allerdings hat die Ausgestaltung dieser Befugnisse Rückwirkungen auf die Funktion und das Ansehen der Kontrollstelle. Es ist unbestritten, dass die Tätigkeitsberichte der Datenschutzbeauftragten, in denen sie Missstände im Datenschutz dokumentieren, eine große politische Wirkung erzielen und zu Verbesserungen im Datenschutz führen. Auch sollte von deren engen Anbindung an die Parlamente, die ihnen zusätzliches politisches Gewicht verleiht, gerade nicht abgerückt werden. Indes wird die Spannung zwischen Beratung und Sanktion, die bisher und auch in Zukunft im Wesentlichen die Kontrollaufgaben im nicht öffentlichen Bereich betrifft, nicht dadurch gelöst, dass beide Bereiche trotz der oben beschriebenen Notwendigkeiten voneinander getrennt bleiben. Überdies entspricht es Art. 19 Abs. 4 GG, dass sich Adressaten von Verwaltungsentscheidungen gerichtlich gegen diese zur Wehr setzen können. Keine andere unabhängige Behörde gilt in ihrer Unabhängigkeit als geschwächt, wenn sie vor Gerichten ihre Auffassung zu vertreten hat. Selbst der Bundestag unterliegt in seinen Entscheidungen der richterlichen Prüfung durch das Bundesverfassungsgericht. Die Befürchtung, von Entscheidungen der Datenschutzbeauftragten Betroffene würden von ihrem Recht auf richterliches Gehör Gebrauch machen, kann daher kein Grund sein, an der zweigleisigen Kontrolle des öffentlichen und nicht öffentlichen Datenschutzes festzuhalten. Unabhängigkeit und gerichtliche Überprüfungsmöglichkeit sind ohne weiteres miteinander vereinbar, wie die DSRL in Art. 28 zeigt, indem sie den *unabhängigen* Kontrollstellen administrative Rechte zubilligt.[948] Die bisherige Praxis im nicht öffentlichen Bereich, in der Zwangsmittel nur als ultima ratio Anwendung fanden, zeigt, dass die Befürchtung, es komme zu einer Flut von gerichtlichen Verfahren, nicht empirisch zu untermauern ist. In der Regel werden Meinungsverschiedenheiten bereits außergerichtlich beigelegt. Nur in sehr wenigen Fällen kam es zu einem Gerichtsverfahren. Außerdem haben die Landesdatenschutzbeauftragten, die Funktionen der Aufsichtsbehörde im nicht öffentlichen Bereich wahrnehmen, weder ihre Unabhängigkeit noch ihr öffentliches Ansehen eingebüßt – ganz im Gegenteil.

Die Sonderzuständigkeiten im Bereich der Telekommunikation, bei Mediendiensten und Rundfunkanstalten müssen weitestgehend aufgegeben werden. Sie sind der althergebrachten Struktur in diesen Bereichen geschuldet, die in der Vergangenheit von öffentlich-rechtlichen Institutionen dominiert wurden. Angesichts der drastischen organisatorischen Veränderungen im Telekommunikations-, Medien- und Rundfunkbereich sind sie nicht mehr zeitgemäß. Lediglich für den journalistisch-redaktionellen Bereich werden im Hinblick auf die grundrechtlich garantierte Pressefreiheit nach Art. 5 GG und die Rechtsprechung des Bundesverfassungsgerichts hierzu auch in Zukunft eigenständige Datenschutzbeauftragte der Rundfunkanstalten für die Einhaltung datenschutzrechtlicher Regelungen vorzusehen sein.

9.1.2 Unabhängigkeit der öffentlichen Kontrollstellen

Die Unabhängigkeit der Kontrollbehörden für den Datenschutz ist einer der zentralen Punkte für die Effizienz und die öffentliche Akzeptanz der Tätigkeit der Datenschutzbeauftragten des Bundes und der Länder. Sowohl im Europäischen Rahmen als auch in der deutschen höchstrichterlichen Rechtsprechung kommt dies zum Ausdruck. So betont die europäische Daten-

[948] *Dammann/Simitis*, Art. 28 Rn. 6.

schutzrichtlinie in Art. 28 Abs. 1 die „völlige Unabhängigkeit“ öffentlicher Kontrollstellen bei der Wahrnehmung ihrer Aufgaben und bezeichnet diese Behörden in Erwägungsgrund 62 als „wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten“. Das Bundesverfassungsgericht unterstreicht wiederum die „erhebliche Bedeutung“ unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.[949] Nicht zuletzt diese höchstrichterliche Einordnung der Datenschutzbeauftragten als Garanten eines zentralen Grundrechts unterstreicht die Notwendigkeit, der Unabhängigkeit der Beauftragten ein besonderes Augenmerk zu widmen.

Der Streit um die richtige Rechtsstellung der Beauftragten für den Datenschutz – und um diese geht es vor allem bei der Frage nach deren Unabhängigkeit – wird ebenso lange geführt, wie es Datenschutzgesetze in Deutschland gibt. Unterschiedliche verfassungsrechtliche Auffassung hinsichtlich der Vereinbarkeit der Rechtsstellung der Beauftragten mit dem Prinzip der Gewaltenteilung auf der einen, und der Wunsch, eine effiziente Wahrnehmung der Aufgaben und eine größtmögliche öffentliche Akzeptanz der Datenschutzbeauftragten sicherzustellen, auf der anderen Seite, haben dazu geführt, dass der Bund und die Länder bei der Ausgestaltung der Rechtsstellung der Beauftragten sehr unterschiedliche Wege wählten: als obere Bundes-/Landesbehörde, die der Rechts- und/oder Dienstaufsicht der gesamten Regierung oder eines Ministers unterliegt (Bund), als oberste Landesbehörde, die keiner Dienst- oder Rechtsaufsicht unterliegt (Rheinland-Pfalz) oder die unter der Dienstaufsicht des Parlamentspräsidenten (Berlin) steht, als Vorstand einer rechtsfähigen Anstalt des öffentlichen Rechts mit Dienstherrenfähigkeit, der den Ministerpräsidenten oder die Ministerpräsidentin zum Dienstvorgesetzten hat und der Rechtsaufsicht des Innenministeriums nur insoweit unterliegt, als seine Kontrolltätigkeit im nicht öffentlichen Bereich betroffen ist (Schleswig-Holstein).

Die (völlige) Unabhängigkeit der Kontrollstellen im Sinne der Richtlinie wird in den verschiedenen Jurisdiktionen in Deutschland – soweit die Richtlinie in den aktuellen Gesetzen bereits berücksichtigt wurde – offensichtlich sehr unterschiedlich interpretiert.

In der zweiten Stufe der Novellierung des Datenschutzrechts sollte die Beibehaltung der Rechtsaufsicht über die Kontrollstellen sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich aus europarechtlichen Erwägungen wie auch aus grundsätzlichen datenschutzpolitischen Gründen grundlegend überdacht werden.

Die in Art. 28 DSRL gewählte Formulierung „völlige Unabhängigkeit“ impliziert eindeutig, dass die Richtlinie keine auch noch so geringe Abhängigkeit der Kontrollstellen toleriert.[950] Selbst ein Formulierungsvorschlag der Bundesrepublik während des Entstehungsprozesses der Richtlinie, der eine Unabhängigkeit nur gegenüber der zu kontrollierenden Stelle vorsah – was eine Selbstverständlichkeit darstellen dürfte –, wurde von den anderen Mitgliedsstaaten abgelehnt.[951] Art. 28 Abs. 1 DSRL sieht eine funktionale Unabhängigkeit vor, die die Einflussnahme auf die Meinungsbildung und das Vorgehen der Kontrollstellen unmöglich macht.[952]

Rechtsaufsicht, also die Aufsicht über die Rechtmäßigkeit der Tätigkeit der öffentlichen Kontrollstellen, ist mit einer völligen Unabhängigkeit und Weisungsfreiheit unvereinbar.[953] Rechtsaufsicht ist nur dann sinnvoll, wenn sie der aufsichtsführenden Instanz die Möglichkeit bietet, ihre Rechtsauffassung gegenüber der des zu Beaufsichtigenden durchzusetzen. Dies

---

949 *BVerfGE* 65, 1 (46).

950 *Bäumler*, DuD 2000, 20.

951 *Dammann/Simitis*, Art. 28 Rn. 6; *Ehmann/Helfrich*, Art. 28 Rn. 6.

952 *Dammann/Simitis*, Art. 28 Rn. 6; *Ehmann/Helfrich*, Art. 28 Rn. 6.

953 *Mitrou* 1993, 71f.

aber ist die klassische Einflussnahme auf das Handeln einer Behörde. Der Einschnitt in die Unabhängigkeit ist bezogen auf die Kontrolle im öffentlichen Bereich um so gravierender, als für den Bundesbeauftragten die Rechtsaufsicht der Bundesregierung besteht, welche gerade Ziel der Kontrolltätigkeit ist: „Der zu Kontrollierende kontrolliert den Kontrolleur".

Auch die ursprüngliche – nunmehr erweiterte – Intention des Datenschutzes, nämlich die Bürgerinnen und Bürger vor einem alles wissenden Staat zu schützen, kann nur durch eine von diesem völlig unabhängige Stelle durchgesetzt werden. Im Übrigen haben alle Landesdatenschutzgesetze auf eine Rechtsaufsicht über die Datenschutzbeauftragten in ihrer Funktion als Kontrollstellen für den öffentlichen Bereich verzichtet.

Neben diese Erwägungen tritt ein weiterer Aspekt, der den nicht öffentlichen Bereich betrifft: Die erste Stufe der Novellierung des BDSG hat bereits – in Umsetzung der europäischen Richtlinie – von der anlassbezogenen Kontrolltätigkeit der Aufsichtsbehörden Abschied genommen. Angesichts der fortschreitenden Vernetzung von Dateien war dieser Schritt unausweichlich. Damit werden den Aufsichtsbehörden zum Schutz der Grundrechte der von der Datenverarbeitung betroffenen Bürgerinnen und Bürger nun durch das BDSG weitreichende Kontrollbefugnisse gegenüber privaten Stellen zugestanden, die ihrerseits wiederum Träger von Grundrechten sind. Dieser Eingriff in die Grundrechtssphäre kann aber nur gerechtfertigt sein, wenn sichergestellt wird, dass der im Interesse eines effektiven Grundrechts- (Daten)schutzes von den Kontrollstellen erlangte Zugang zu Informationen auf diese beschränkt bleibt.

Rechtsaufsicht wird nur dann sinnvoll ausgeübt, wenn die Aufsicht führende Instanz uneingeschränkten Einblick in die Tätigkeit des Datenschutzbeauftragten, mithin auch in die dabei erlangten Informationen hat. Im Rahmen der Rechtsaufsicht würde somit der Staat Informationen erlangen, die nur um deren Schutz vor unberechtigter Kenntnisnahme willen durch die Kontrollstellen gesammelt wurden. Diese Verkehrung der Zielrichtung des Datenschutzes kann nur durch die Aufgabe der Rechtsaufsicht der Exekutive verhindert werden.[954] Je weniger der private Bereich die Kontrollstellen als verlängerten Arm der Exekutive mit ihren spezifischen Interessen begreift, um so größer wird darüber hinaus die Akzeptanz und Bereitschaft zur Zusammenarbeit mit den öffentlichen Datenschutzbeauftragten sein.

Verfassungsrechtliche Bedenken unter den Schlagworten „ministerialfreier Raum" und „vierte Gewalt" erscheinen unberechtigt. Zwar ist die Einordnung der Datenschutzbeauftragten in die Trias der Gewaltenteilung – zumindest dort, wo sie, wie bisher fast ausschließlich, keine oder kaum exekutive Befugnisse besitzen – tatsächlich schwierig und spiegelt die Einzigartigkeit der Aufgabe des Datenschutzes wider: Sie sind nicht Teil der Legislative und haben auch keine judikativen Befugnisse, sind vielmehr regelmäßig als Verwaltungsbehörde organisiert. Somit liegt auch eine Einordnung in den exekutiven Bereich der Staatsgewalt nahe. Andererseits liegt der Schwerpunkt ihrer Tätigkeit in der Kontrolle der Exekutive, was sie – zumindest partiell – inhaltlich in die Nähe zur Legislative und Judikative rücken lässt – ohne über deren spezielle Befugnisse zu verfügen. Die Unabhängigkeit der Datenschutzbeauftragten ist heute schon an der richterlichen Unabhängigkeit ausgerichtet.

Selbst wenn man aber die Datenschutzbeauftragten als Teil der Exekutive begreift, ist daraus nicht zwingend zu schlussfolgern, dass sie unter der Rechtsaufsicht der Exekutive zu stehen haben. Das Bundesverfassungsgericht hat ausdrücklich festgestellt, dass „ministerialfreie Räume" nicht grundsätzlich unzulässig sind:[955] Die Übertragung von Verwaltungsaufgaben auf von Regierung und Parlament (!) unabhängige Stellen ist nur dort nicht zulässig, wo die wahrzunehmenden Regierungsaufgaben von solcher politischen Tragweite sind, dass es durch

[954] S. Stellungnahme des *Hessischen Datenschutzbeauftragten* zur BDSG-Novellierung vom 30.6.1997.

[955] S. auch *Bizer*, DuD 1997, 481.

den Entzug der Aufgabe der Regierung unmöglich gemacht würde, die von ihr geforderte Verantwortung zu tragen. Würde dies geschehen, so bestünde die Gefahr, dass unkontrollierte und niemand verantwortliche Stellen Einfluss auf die Staatsverwaltung gewinnen würden.[956] Die Einrichtung völlig unabhängiger Kontrollstellen aber entzieht der Regierung für den öffentlichen Bereich gerade nicht ihre Verantwortung für die Einhaltung des Datenschutzes („Selbstkontrolle"), sondern ergänzt ihre originäre Pflicht, dieser Verantwortung nachzukommen, durch ein zusätzliches Korrektiv („Fremdkontrolle"). Überdies wären die Datenschutzbeauftragten in beiden Bereichen der Legislative gegenüber verantwortlich. Im Rahmen der Aufsicht über den nicht öffentlichen Bereich ist als weiteres Korrektiv der Verwaltungsrechtsweg auch heute schon eröffnet.

Einem Verzicht auf die Rechtsaufsicht über die öffentlichen Datenschutzbeauftragten stünde auch das Demokratieprinzip aus Art. 20 Abs. 2 GG nicht entgegen. Dieses verlangt für die Ausübung staatlicher Gewalt eine demokratische Legitimation durch das Volk als Quelle aller Staatsgewalt, sobald sich die Tätigkeit als partizipatorisches Verwaltungshandeln darstellt und nicht lediglich vorbereitend oder konsultativ zum tatsächlichen Verwaltungshandeln steht.[957] Insoweit ist die Tätigkeit der öffentlichen Datenschutzbeauftragten bereits heute – ohne die noch zu behandelnden exekutiven Befugnisse, mit denen sie ausgestattet werden sollten – Ausübung staatlicher Gewalt, die einer demokratischen Legitimation bedarf. Diese Legitimation wird bereits heute in allen Datenschutzgesetzen durch die direkt vom Volk gewählten Parlamente hergeleitet. Ihre Bestandteile sind eine funktionelle Legitimation durch eine gesetzliche Regelung der Aufgaben und Befugnisse des Datenschutzbeauftragten, eine personelle Legitimation durch deren Wahl durch das Parlament und eine sachlich-inhaltliche durch Kontroll- und Berichtspflichten gegenüber dem Parlament.[958]

Wenn die Einbindung der Datenschutzbehörden in die Exekutive auch nicht per se gegen die europäische Datenschutzrichtlinie verstößt,[959] so ist es gleichwohl – um jeglichen Anschein einer Abhängigkeit zu vermeiden – wünschenswert, die Kontrollstellen generell als oberste Bundes- und Landesbehörden einzurichten.[960] Insoweit könnte auf die Modelle der Landesdatenschutzbehörden in Berlin, Rheinland-Pfalz und Hessen zurückgegriffen werden. Nach der Rangstufe ist der Bundesbeauftragte bereits jetzt durch die unmittelbare Zu- aber nicht Unterordnung zum Bundesminister des Innern oberste Bundesbehörde.[961] Eine solche organisatorische Klarstellung würde auch die komplizierten Erwägungen hinsichtlich einer Rechtsaufsicht obsolet werden lassen.

Die von einzelnen Experten in den Fachgesprächen zur Vorbereitung dieses Gutachtens angeregte generelle Abwahlmöglichkeit der Datenschutzbeauftragten durch die Parlamente, als Stärkung der parlamentarischen Legitimation, sollte nicht vorgesehen werden. Sie liefe der Unabhängigkeit der Datenschutzbeauftragten zuwider.

9.1.3 Befugnisse, Aufgaben

Befugnisse und Aufgaben der Datenschutzbeauftragten müssen der qualitativen und quantitativen Entwicklung der Datenverarbeitung sowohl im öffentlichen wie auch im nicht öffentlichen Bereich Rechnung tragen. Sie sind an den Zielsetzungen des Datenschutzes[962] auszurichten, müssen die verschiedenen Elemente des Datenschutzsystems in der Bundesre-

---

956 *BVerfGE* 9, 268 (282).

957 *BVerfGE* 83, 60 (74).

958 S. *BVerfGE* 93, 37 (66 ff.); *Bizer*, DuD 1997, 482.

959 *Damann/Simitis*, Einl., Rn. 40.

960 *Tinnefeld/Ehmann*, CR 1989, 637, 641.

961 *Dammann*, in: *Simitis u.a.*, BDSG, § 22 Rn. 22.

962 S. Teil 2 Kap. 1.

publik Deutschland berücksichtigen und sich an den Prinzipien einer modernen, effizienten Verwaltung orientieren.

Das hinsichtlich des Aufgabenspektrums und der Kontrollbefugnisse bewährte System der Datenschutzaufsicht leidet von Anfang an – sowohl im öffentlichen als auch im nicht öffentlichen Bereich – an mangelnden Durchsetzungskompetenzen. Das BDSG hat mit der Normierung von neuen Ordnungswidrigkeitstatbeständen einen ersten Schritt getan. Gleichwohl fehlt es nach wie vor an Durchsetzungsmöglichkeiten im Verwaltungsverfahren. Weiter reichende exekutive Befugnisse sollen die bisher im Vordergrund stehende Beratungs- und Servicefunktion der staatlichen Datenschutz-Kontrollbehörden nicht ersetzen. Im Gegenteil: Dadurch dass die datenverarbeitenden Stellen bei Verstößen gegen datenschutzrechtliche Regeln und nachhaltiger Beratungs- und Ermahnungsresistenz mit Sanktionen rechnen müssen, wird sich ihre Bereitschaft erhöhen, Beratung zu suchen.[963]

Schon im Sinn der Europäischen Datenschutzrichtlinie, die den Datenschutzbehörden „wirksame Einwirkungsbefugnisse" zuordnet, müssen den Datenschutzinstanzen exekutive Befugnisse eingeräumt werden. Sie unterscheidet dabei im übrigen nicht zwischen dem öffentlichen und dem nicht öffentlichen Bereich. Zwar sind die Mitgliedstaaten nicht verpflichtet, die in Art. 28 Abs. 3 DSRL aufgeführten Befugnisse ausnahmslos zu übernehmen, allerdings sollte ein modernes deutsches Datenschutzrecht sie vollständig ausschöpfen:

Die Untersuchungsbefugnisse nach Art. 28 Abs. 3, 1. Spiegelstrich DSRL sind durch die entsprechenden Regelungen der §§ 24, 38 BDSG gewährleistet.

Eine Anzeigebefugnis nach Art. 28 Abs. 3, 3. Spiegelstrich DSRL besteht bei Verstößen im nicht öffentlichen Bereich nach der Neufassung von § 38 Abs. 1 Satz 5 BDSG.

Wirksame Einwirkungsbefugnisse gemäß Art. 28 Abs. 3, 2. Spiegelstrich DSRL beschränken sich nach § 38 Abs. 5 BDSG bisher auf den nicht öffentlichen Bereich und dort auf die Anordnung von Maßnahmen zur Beseitigung technisch-organisatorischer Mängel und der Untersagung des Einsatzes bestimmter Verfahren nach erfolgloser Zwangsgeldfestsetzung – jedoch nur, wenn diese an schwerwiegenden Mängeln leiden und mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind. Im öffentlichen Bereich belaufen sich die Befugnisse der Kontrollstellen auch nach der BDSG-Novellierung auf Beanstandungs-, Beratungs- und Berichtskompetenzen. Befugnisse, eine Sperrung, Löschung oder Vernichtung von Daten anzuordnen, bestehen nicht. Ebenso fehlt es an einem Sanktionsinstrument, diese durchzusetzen.

Die Beachtung datenschutzrechtlicher Bestimmungen ist für Behörden nach dem Grundsatz der Gesetzmäßigkeit der Verwaltung eigentlich eine Selbstverständlichkeit. Gleichwohl haben die Gesetzgeber des Bundes und der Länder es für notwendig erachtet, für die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften durch *öffentliche Stellen* Beauftragte für den Datenschutz einzurichten. Eine gewisse Inkonsequenz besteht indes darin, die Datenschutzbeauftragten auf Beratung, Beanstandung und Bericht zu beschränken, und ihnen die Hände zu binden, wenn es um die tatsächliche Abstellung rechtswidriger Datenverarbeitung geht.

Dem Polizei- und Ordnungsrecht ist der Eingriff einer Hoheitsverwaltung in die hoheitliche Aufgabenerfüllung einer anderen wegen des Grundsatzes der Gesetzmäßigkeit der Verwaltung fremd. Diesen Grundsatz wird auch das Datenschutzrecht nicht unberücksichtigt lassen können. In der Regel ist die Datenverarbeitung einer Behörde mit ihrer hoheitlichen Aufgabenerfüllung verbunden, so dass Anordnungsbefugnisse der Kontrollstellen sich auch in Zukunft schwerlich auf den öffentlichen Bereich erstrecken können. Um aber ihren Beanstandungen größeres Gewicht zu verleihen und bei erfolgloser Beratung und Beanstan-

[963] S. zum Konflikt zwischen Beratung und Sanktion: *Weichert* 1998, 223.

dung ein weitergehendes Sanktionsmittel zur Verfügung zu haben, das die Beseitigung der Rechtswidrigkeit der Datenverarbeitung verbindlich regeln könnte, sollte in Erwägung gezogen werden, dass sich die Datenschutzbeauftragten in diesem Fall der Hilfe der Verwaltungsgerichtsbarkeit bedienen können. Entsprechende Verfahren müssten entwickelt werden. Dabei sollte nicht starr an bisherigen Vorgaben des Verwaltungsprozessrechts festgehalten werden, wenngleich möglicherweise auch im Rahmen herkömmlicher rechtswissenschaftlicher Auffassungen Wege dazu gegeben wären. Eine erste Skizze:

Eine Möglichkeit wäre, dass die Datenschutzbeauftragten im Wege einer allgemeinen Leistungsklage die Herstellung der Rechtmäßigkeit der Datenverarbeitung einforderten. Dadurch würden sie selbst nicht in die hoheitliche Aufgabenerfüllung einer anderen Behörde eingreifen, deren Rechtsverstoß gleichwohl einer richterlichen Prüfung unterworfen. Die Datenschutzbeauftragten könnten so, entsprechend dem in Art. 28 Abs. 3 3. Spiegelstrich DSRL vorgesehenen Klagerecht, die Beseitigung von Verstößen gegen datenschutzrechtliche Bestimmungen einklagen. Gleichzeitig würde auch die von Art. 28 Abs. 3 2. Spiegelstrich DSRL geforderte „Wirksamkeit" der Beanstandungen erhöht, da sie – richterlich sanktioniert – die kontrollierten Stellen zu einem Tun oder Unterlassen zwingen würden.[964]

Verfahren, in denen sich als Beteiligte lediglich öffentliche Stellen gegenüber stehen, finden sich im Verwaltungsprozessrecht an verschiedenen Stellen. Häufigste Erscheinungsform solcher „In-sich-Prozesse" sind Organstreitverfahren mit kommunalverfassungsrechtlichem Hintergrund. Aber auch Behörden oder Behördenleiter sind mit einer verwaltungsgerichtlichen Klagebefugnis ausgestattet.[965]

Einem solchen Verfahren könnte nicht entgegengehalten werden, dass der Datenschutzbeauftragte keine eigenen Rechte (individuelle Klagebefugnis) geltend macht. Das Verwaltungsprozessrecht zielt zwar vorrangig auf den Schutz von Rechtspositionen des Einzelnen und schließt grundsätzlich die Verfolgung öffentlicher Interessen aus. Gleichwohl kennt es auch Ausnahmen, soweit Landes- oder Bundesgesetze dies ausdrücklich zulassen.[966] Die bekannteste Durchbrechung des Grundsatzes des Individualrechtsschutzes im Verwaltungsprozessrecht sind altruisitsche Verbandsklagebefugnisse im Naturschutzrecht. Aber auch dem Bundesbeauftragte für Asylangelegenheiten ist beispielsweise nach § 6 Abs. 2 Satz 3 AsylVfG eine Klagebefugnis ohne eine eigene Betroffenheit zugebilligt. Gegen Entscheidungen des Bundesamts für die Anerkennung ausländischer Flüchtlinge kann er Klage erheben. Die Funktion des Bundesbeauftragen für die Anerkennung ausländischer Flüchtlinge unterscheidet sich zwar von der des Bundesdatenschutzbeauftragten, da er als Vertreter des öffentlichen Interesses die staatlichen Belange im Asylverfahren zur Geltung bringt und dabei der Weisungen des Bundesinnenministeriums unterliegt.[967] Gleichwohl greift er die Entscheidung einer Bundesbehörde an. Beklagter ist die Bundesrepublik Deutschland, vertreten durch den Leiter des Bundesamts.[968]

Stellt man im Bereich der Kontrolle der öffentlichen Stellen auf die Ombudsmann-Funktion des Bundesbeauftragten für die Interessen der Betroffenen ab, so ließen sich ebenfalls Parallelen zur Funktion der Verbände ziehen, die das öffentliche Interesse beispielsweise am Landschafts- und Naturschutz unabhängig vom Individualinteresse einzelner Betroffener verfolgen. Eine solche Funktion könnte der Datenschutzbeauftragte als Klageberechtigter

964 *Giesen*, DuD 1997, 230.

965 *Kopp/Schenke*, § 63, Rn. 6, z.B.: § 6 Abs. 2 Satz 3 AsylVfG.

966 *Kopp/Schenke*, § 42 Rn. 180 ff.

967 *Marx* 1999, § 6 Rn. 1, 4.

968 *Marx* 1999, § 6 Rn. 18.

gegen rechtswidrige Verarbeitung personenbezogener Daten durch öffentliche Stellen ausfüllen.

Will man indes die letzte Entscheidung über eine Einstellung des streitigen Datenverarbeitungsverfahrens nicht dem Gericht sondern der Behörde selbst überlassen, so wäre an eine Art Feststellungsklage des Datenschutzbeauftragten zu denken, die auf die Feststellung zielt, dass das konkrete Datenverarbeitungsverfahren rechtswidrig ist. Um in diesem Fall eine klassische verwaltungsrechtliche Feststellungsklage zu ermöglichen, wäre gegebenenfalls § 43 VwGO entgegen der bisherigen allgemeinen Auffassung, dass die rechtliche Qualifikation bestimmter Vorgänge nicht feststellungsfähig sei,[969] neu auszulegen. Es sei in diesem Zusammenhang allerdings darauf hingewiesen, dass das *VG Hamburg* in Anlehnung an eine Entscheidung des Bundesverwaltungsgericht[970] davon ausging, dass „der Begriff des Rechtsverhältnisses weit ausgelegt wird. Als feststellungsfähiges Rechtsverhältnis werden auch einzelne Berechtigungen und Verpflichtungen angesehen."[971] Bezogen auf ein rechtswidriges Datenverarbeitungsverfahren bedeutet dies, dass die Verpflichtung zu dessen Einstellung aufgrund der Rechtswidrigkeit feststellungsfähiges Rechtsverhältnis im Sinne des § 43 Abs. 1 1. Alt. VwGO darstellt. Überdies betrifft eine rechtswidrige Datenverarbeitung immer auch ein Rechtsverhältnis – wenngleich nicht das zwischen der verantwortlichen Stelle gegenüber dem Datenschutzbeauftragten, sondern gegenüber dem Betroffenen – da die Behörde zum Schutz der informationellen Selbstbestimmung des Betroffenen für eine rechtmäßige Verarbeitung seiner personenbezogenen Daten Sorge tragen muss.

Die Kontrollstellen müssen mit der Befugnis ausgestattet werden, gegenüber *nicht öffentlichen Stellen* die Sperrung, Löschung oder Vernichtung von Daten, die widerrechtlich verarbeitet wurden, durch bindenden Verwaltungsakt anzuordnen. Bei Verletzung der Grundsätze der Datenverarbeitung[972] sollte ihnen ein zweistufiges Instrumentarium in die Hand gegeben werden: Ein vorläufiges Verbot der Datenverarbeitung wird angeordnet, das bis zur Beseitigung der Mängel, die mit einer Frist verbunden wird, gilt. Bei wiederholter Verletzung oder erfolglosem Ablauf der Frist zur Herstellung der Voraussetzungen einer rechtmäßigen Datenverarbeitung wird ein endgültiges Verbot ausgesprochen. Dabei dürfen sich Anordnungsbefugnisse nicht nur auf schwerwiegende Mängel i.S.d. § 38 Abs. 5 Satz 2 BDSG beschränken. Ein effektives Instrument, datenverarbeitende Stellen zur Datenverarbeitung nach den gesetzlich geregelten Grundsätzen anzuhalten, ist darüber hinaus eine in Art. 28 Abs. 3 2. Spiegelstrich DSRL vorgesehene Verwarnung oder Ermahnung an den für die Verarbeitung Verantwortlichen. Zu erwägen wäre, eine solche Verwarnung in geeigneter Weise unabhängig von den Tätigkeitsberichten öffentlich bekannt zu machen.

Um darüber hinaus auch eine effektive strafrechtliche Ahndung von Verstößen gegen den Datenschutz zu ermöglichen, sollten die Kontrollstellen in Zukunft über eine umfassende Strafantragsbefugnis verfügen. Landesrechtliche Regelungen wie beispielsweise in Berlin[973] könnten hier als Vorbild dienen. Datenschutzstraftaten generell als Offizialdelikt vorzusehen[974] erscheint nicht ratsam. Strafverfolgung, die den rein privaten Bereich betrifft, sollte auch in Zukunft grundsätzlich vom Verhalten des Verletzten abhängig gemacht werden. Straftaten, deren Verfolgung darüber hinaus – beispielsweise wegen der Schwere der Tat, dem dadurch entstandenen Schaden oder der öffentlichen Wirkung – im öffentlichen Interesse liegt, können die Datenschutzbeauftragten durch ihre Antragsbefugnis gegenüber den Ermitt-

969 *Kopp/Schenke*, § 43 Rn. 13.
970 *BVerwGE* 36, 218 (225).
971 *VG Hamburg*, GewA 1981, 261.
972 S. Teil 3 Kap. 3.
973 § 32 Abs. 3 Satz 3, 4 BlnDSG.
974 So *Weichert*, NStZ 1999, 492.

lungsbehörden anzeigen. Insoweit können sie korrigierend eingreifen, indem die Initiative zur Strafverfolgung in diesen Fällen nicht allein den Betroffenen oder der Staatsanwaltschaft, für die das Datenschutzrecht ohnehin eher ein „exotisches“ Nebengebiet ist, überlassen wird. Überdies wird durch eine Strafantragsbefugnis der öffentlichen Kontrollstellen der Tatsache Rechnung getragen, dass die Verletzten häufig von ihrer Antragsberechtigung keine Kenntnis haben oder die dreimonatige Antragsfrist nach § 77b StGB bereits abgelaufen ist. Für die Datenschutzbehörden beginnt diese Frist erst mit ihrer Kenntnis des Verstoßes.

Schließlich könnte für Personen, die durch die Nichtbeachtung datenschutzrechtlicher Vorschriften eine Ordnungswidrigkeit oder Straftat begangen haben, ein Datenschutzunterricht eingerichtet werden. Auf Vorladung der Kontrollstellen, durchgeführt entweder durch diese selbst oder durch die Industrie- und Handelskammer, könnten so Kenntnisse im Datenschutz vermittelt und auf die Auswirkungen von Verstößen gegen datenschutzrechtliche Bestimmungen auf die informationelle Selbstbestimmung aufmerksam gemacht werden. Eine entsprechende Vorschrift weist in ihrer Erziehungsfunktion Parallelen zu § 48 StVO auf und ist auch im Entwurf zum UGB vorgeschlagen worden.[975]

Führt die Verletzung von Datenschutzpflichten (z.B. Nichtbestellen eines Datenschutzbeauftragten) zu unrechtmäßigen Vermögensvorteilen (z.B. ersparte Kosten), die nicht von einer betroffenen Person geltend gemacht werden können, sollte die Kontrollstelle nach pflichtgemäßem Ermessen diesen Gewinn abschöpfen können.

Die in Art. 28 Abs. 2 DSRL vorgesehene Anhörung der Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten sollte ausdrücklich im BDSG erwähnt werden. § 26 Abs. 3 BDSG muss die Verpflichtung der entsprechenden Stellen zur Konsultation des Bundesbeauftragten enthalten.

Schließlich sollten die Datenschutzbeauftragten bei der *Selbstregulierung* mitwirken. Entsprechend den vorgeschlagenen Regelungen[976] obliegt ihnen die Überprüfung und Anerkennung von Verhaltensregeln, die sich die verantwortliche Stellen oder ihre Vereinigungen selbst gegeben haben.

9.2 Behördliche und betriebliche Datenschutzbeauftragte

Sowohl auf der Sitzung der Begleitkommission als auch in allen Fachgesprächen[977] wurde eine Stärkung der Rolle der betrieblichen und behördlichen Datenschutzbeauftragten angemahnt. Insbesondere seien Maßnahmen zur Verbesserung ihrer Qualifikation zu treffen und die Anforderungen an zu bestellende Datenschutzbeauftragte hinsichtlich ihrer Fachkunde präziser zu formulieren. Es wurde vorgeschlagen, sie auch als Beschwerdeinstanz in Datenschutzfragen innerhalb des Unternehmens oder der Behörde vorzusehen.[978] Die Verbesserung des Kündigungsschutzes und eine Vorgabe hinsichtlich des Zeitrahmens der Tätigkeit als Datenschutzbeauftragter entsprechend der Größe des Unternehmens und der Art seiner Tätigkeit wurden wiederholt angesprochen.

Bereits die BDSG-Novellierung hat die Bedeutung betrieblicher und behördlicher Datenschutzbeauftragter deutlich erhöht. Ihnen kommt eine zentrale Rolle bei der Sicherstellung des Datenschutzes zu. Sie sind schon jetzt ein Element der Selbstregulierung und dokumentie-

---

975 § 65 UGB-E: „Wer umweltrechtliche Vorschriften nicht beachtet und sich dabei ordnungswidrig verhält oder eine Straftat gegen die Umwelt begeht, ist auf Vorladung der zuständigen Behörde verpflichtet, an einem Unterricht über umweltgerechtes Verhalten teilzunehmen.“, UGB-KOM-E 1998, 132, 565.

976 S. Teil 3 Kap. 6.4.

977 S. die Zusammenfassungen in Anhang 3 und 4, S. 248 ff.

978 S. hierzu ausführlich Teil 3 Kap. 7.2.

ren die Kooperation von Staat und privatem Bereich im Datenschutz.[979] Die Privilegierung verantwortlicher Stelle, die betriebliche oder behördliche Datenschutzbeauftragte bestellen (müssen),[980] unterstreicht deren besondere Bedeutung im System des Datenschutzes. Spiegelbildlich zur Unabhängigkeit der öffentlichen Datenschutzbeauftragten und Aufsichtsbehörden muss die Unabhängigkeit der behördlichen und betrieblichen Datenschutzbeauftragten bei der Gewährleistung des internen Datenschutzes weiter gestärkt werden.

Die bisher bereits festgeschriebene Weisungsfreiheit muss beibehalten werden. Darüber hinaus dürfen der Zusammenarbeit mit den externen Datenschutzbehörden keinerlei Hindernisse in den Weg gelegt werden. So muss auch der behördliche Datenschutzbeauftragte in Zweifelsfällen aus eigener Entscheidung heraus den Bundesbeauftragten oder die Aufsichtsbehörde konsultieren können. Dieses Instrument hat eine zweifache Funktion. Zum Einen dient es dem Datenschutzbeauftragten, bei Unsicherheiten die Beratung der Kontrollstelle zu suchen. Zum Anderen wird auf diese Weise die Kontrollstelle bei Meinungsverschiedenheiten zwischen dem Datenschutzbeauftragten und der Leitung der verantwortlichen Stelle in ihrer Schlichtungsfunktion[981] eingeschaltet und kann ihrer Aufgabe, der Überprüfung der Einhaltung von Vorschriften über den Datenschutz, nachkommen. Die Regelung des § 4g Abs. 1 Satz 3 BDSG, nach der die oberste Bundesbehörde entscheiden soll, ob sich der behördliche Datenschutzbeauftragte an den Bundesbeauftragten in einem Zweifelsfall wenden darf, sollte aufgehoben werden.

Diese zusätzliche Hürde zur Anrufung des Bundesbeauftragten widerspricht im übrigen auch den in § 24 BDSG vorgesehenen umfangreichen Kontrollbefugnissen des Bundesbeauftragten in den öffentlichen Stellen des Bundes: Der Bundesbeauftragte kann ohnehin seine Kontrolltätigkeit kraft eigener Befugnis auf die Bereiche erstrecken, in denen zwischen dem Leiter einer Behörde und dem zuständigen behördlichen Datenschutzbeauftragten Unstimmigkeiten bestehen. Bestehen Meinungsverschiedenheiten in einer Behörde, so ist die Kontroll- und Beratungstätigkeit des Bundesbeauftragten um so mehr gefragt. Sollten sich die Auffassungen des behördlichen Datenschutzbeauftragten, denen der Leiter der Behörde widerspricht, als nicht stichhaltig herausstellen, so wird der Bundesbeauftragte dies feststellen und dem Ansinnen nicht weiter nachgehen. Dies hat aufgrund der Verschwiegenheitsverpflichtung des Bundesbeauftragten auch keinerlei weitere Auswirkungen. Stellt sich aber heraus, dass der Vorgang, mit dem sich der behördliche Datenschutzbeauftragte an den Bundesbeauftragten wendet, tatsächlich von Belang ist und datenschutzrechtliche Konsequenzen hat, so sollte der Leiter der Behörde durch sein Veto nicht eine Befassung des Bundesbeauftragten mit dem Vorgang verhindern können. Dies stünde im Gegensatz zur gewünschten Effizienz des Datenschutzes im öffentlichen Bereich. Interessant ist insoweit, dass diese Vorschrift für den privaten Bereich nicht gilt. Ein weitergehender Eingriff in die Verantwortung des Leiters einer Behörde als dieser ohnehin durch die Kontrolltätigkeit des Bundesbeauftragten gesetzlich schon vorgesehen ist,[982] ist nicht ersichtlich. Sollten Bedenken bestehen, dass der behördliche Datenschutzbeauftragte sich durch dieses direkte Anrufungsrecht innerhalb der Behörde verselbständigt, so könnte eine Informationspflicht über eine Kontaktaufnahme mit dem BfD vorgesehen werden. Der Weisungsungebundenheit widerspricht aber, dass der behördliche Datenschutzbeauftragte sich mit dem BfD nicht in Verbindung setzen darf, ohne zuvor die Genehmigung des Leiters der Behörde einzuholen. Die Anrufung des Bundesbeauftragten als Kontroll- und Fachinstanz ist ein zentrales Instrument des Datenschutzes. Gerade für dieses

---

979 S. Teil 2 Kap. 3.5.

980 S. die entfallende Meldepflicht nach § 4d BDSG.

981 *Bergmann/Möhrle/Herb*, § 37 Rn. 14.

982 „Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Bediensteten bei der Erfüllung ihrer Aufgabe zu unterstützen“ (§ 24 Abs. 4 BDSG).

Instrument aber die Weisungsfreiheit des behördlichen Datenschutzbeauftragten aufzuheben, erscheint kontraproduktiv.

Untrennbar mit der Weisungsfreiheit und damit der Unabhängigkeit des Datenschutzbeauftragten ist die Frage eines effektiven Kündigungsschutzes verbunden. § 4f Abs. 3 Satz 4 BDSG lässt eine Kündigung der Bestellung in entsprechender Anwendung des § 626 BGB zu und hat damit die alte Regelung des BDSG 1990 übernommen. Dass dieser Kündigungsschutz nicht ausreichend ist, mithin die Unabhängigkeit des Datenschutzbeauftragten gefährdet, zeigen die unterschiedlichen Auffassungen[983] über seine Tragweite und die Rechtsprechung.[984] Nach einer Auffassung bezieht sich die Regelung des § 4f Abs. 3 Satz 4 BDSG (§ 36 Abs. 3 Satz 4 a.F.) allein – und unabhängig von anderen Tätigkeiten innerhalb des Arbeitsverhältnisses – auf die Funktion als Datenschutzbeauftragter, während sie nach der anderen Auffassung einen umfassenden Schutz des gesamten Arbeitsverhältnisses bietet. Das *LAG Berlin* hat entschieden, dass eine ordentliche Kündigung, soweit sie sich nicht auf die Nebentätigkeit des Arbeitnehmers als Datenschutzbeauftragter bezieht, unter der Voraussetzung, dass sie hinsichtlich der anderweitigen Tätigkeit des Arbeitnehmers innerhalb des Arbeitsverhältnisses gerechtfertigt ist, zulässig sei, auch wenn dies zu einer Beendigung des gesamten Arbeitsverhältnisses führt. Dies hat, wie der damalige Streitfall zeigt, eine Aushöhlung wenn nicht gar ein Leerlaufen des Kündigungsschutzes gemäß § 4f Abs. 3 Satz 4 BDSG zur Folge. Über den Umweg einer ordentlichen Kündigung aufgrund der anderweitigen – in der Regel zeitlich überwiegenden – Tätigkeit kommt es automatisch auch zu einem Widerruf der Bestellung zum Datenschutzbeauftragten trotz der Regelung des § 4f Abs. 3 Satz 4 BDSG. Das LAG Berlin hat zur Untermauerung seiner Auffassung angeführt, der Gesetzgeber hätte, wenn er einen weitergehenden Kündigungsschutz beabsichtigte, eine Regelung vorgesehen, wie sie für den Immissionschutzbeauftragten[985] oder andere Funktionsträger[986] besteht. Die differenziertere Auffassung des *ArbG Berlin*[987] in seiner erstinstanzlichen Entscheidung des Streitfalls, nach der zumindest geprüft werden muss, ob ein Zusammenhang der Kündigung mit der Tätigkeit als Datenschutzbeauftragter nicht auszuschließen ist, unterstreicht indes nur, dass die derzeitige Regelung des Kündigungsschutzes offen für Interpretationen und damit nicht zufriedenstellend ist.

Angesichts der bedeutsamen Funktion, die die betrieblichen Datenschutzbeauftragten bereits jetzt im System des Datenschutzes in Deutschland, das dem Schutz des Grundrechts auf informationelle Selbstbestimmung dient, ausüben, ist es dringend geboten, ihren Kündigungsschutz künftig effektiver zu gestalten und auch für sie einen den Betriebsräten oder Immissionschutzbeauftragten gleichwertigen Schutz vorzusehen, der generell nur eine außerordentliche Kündigung zulässt. Der Entwurf eines UGB hat noch weitergehend den besonderen Kündigungsschutz für betriebliche Umweltbeauftragte auf einen Zeitraum von zwei Jahren (für Betriebsräte gilt eine Ein-Jahres-Frist) nach der Beendigung der Tätigkeit als Umweltbeauftragter ausgedehnt,[988] um dessen Umgehung wirtschaftlich zu erschweren.[989] Eine solche Regelung könnte auch für die betrieblichen und behördlichen Datenschutzbeauftragten in Erwägung gezogen werden.

In diesem Zusammenhang sollte auch die Bestellung externer Datenschutzbeauftragter gemäß § 4f Abs. 2 Satz 2 BDSG genauer geregelt werden. Wiederholt haben Experten in den Fach-

983 S. *Gola/Jaspers*, RDV 1998, 49 m.w.N.

984 *LAG Berlin*, DuD 1998, 413.

985 S. § 58 BImSchG.

986 S. §§ 15 KSchG, 26 Abs. 3 SchwbG.

987 *ArbG Berlin*, Urteil vom 15.4.1997.

988 § 163 Abs. 2 Satz 2 des Entwurfs eines UGB.

989 UGB-KOM-E 1998, 751.

gesprächen darauf hingewiesen, dass auch juristische Personen mit der Wahrnehmung der Funktion des Datenschutzbeauftragten betraut werden. Dadurch aber kann der die Unabhängigkeit des Datenschutzbeauftragten unterstützende Kündigungsschutz umgangen werden, da die juristische Person, die beauftragt wird, eine natürliche Person mit der Funktion des Datenschutzbeauftragten betrauen kann, ohne an § 4f Abs. 3 Satz 4 BDSG gebunden zu sein.[990] Es sollte daher nur die Beauftragung einer natürlichen Person vorgesehen werden, wie dies beispielsweise das Niederländische Datenschutzgesetz[991] in Art. 63 Abs. 1 ausdrücklich vorschreibt. Darüber hinaus sollte auch vorgesehen werden, dass Dienstverträge zur Ausübung der Funktion des Datenschutzbeauftragten einen Mindestzeitraum der Befristung nicht unterschreiten dürfen. Dies würde nämlich ebenso zur Umgehung eines effektiven Kündigungsschutzes führen. Der Bundesverband der Datenschutzbeauftragten Deutschlands (BvD) schlägt einen Zeitrahmen von mindestens fünf Jahren vor.[992]

Wiederholt wird in Literatur und Rechtsprechung auf die besonderen Anforderungen an die fachliche und persönliche Eignung für das Amt des Datenschutzbeauftragten hingewiesen.[993] Gleichwohl begnügt sich das Gesetz nach wie vor mit unbestimmten Begriffen, nach denen die Datenschutzbeauftragten „die erforderliche Fachkunde und Zuverlässigkeit" besitzen müssen. Während sich der Inhalt der erforderlichen Fachkunde zwar noch relativ unproblematisch von den Aufgaben der Datenschutzbeauftragten nach § 4g BDSG herleiten lässt, ist dies bei der Zuverlässigkeit nur hinsichtlich der in § 4f Abs. 4 BDSG festgeschriebenen Verschwiegenheit der Fall. Aus diesem Grunde wäre es wünschenswert, in § 4f BDSG konkrete Aussagen zur fachlichen und persönlichen Qualifikation zu treffen. Insbesondere sollte ausdrücklich festgestellt werden, dass zum Datenschutzbeauftragten derjenige nicht bestellt werden darf, dessen andere betriebsbezogene Aufgaben mit seiner Tätigkeit als Datenschutzbeauftragter in einem Interessenkonflikt stehen würden. Ein Formulierungsvorschlag des Berufsverbandes der Datenschutzbeauftragten Deutschlands zu § 4f BDSG,[994] der als Grundlage für eine gesetzliche Regelung dienen kann, benennt als Qualifikationsmerkmale dem Stand der Technik entsprechende Kenntnisse in der Informationstechnik und die Fähigkeit die datenschutzrechtlichen Vorschriften einschließlich des BDSG anwenden zu können. Möchte man dies in einem BDSG nicht im Einzelnen regeln, so wäre auch an eine Ermächtigung der Bundesregierung zu denken, entsprechend § 55 Abs. 2 Satz 3 BImSchG nach Anhörung der Selbstverwaltungsorganisationen eine Rechtsverordnung zu erlassen, die die Anforderungen an Fachkunde und Zuverlässigkeit näher regeln. Eine solche Regelung hätte den Vorteil, nach der Art der Tätigkeit und der Größe der verantwortlichen Stellen sowie der Sensitivität der verarbeiteten personenbezogenen Daten differenzierte Anforderungen zu beschreiben zu können.[995]

Zur Durchsetzung der Fachkunde käme darüber hinaus eine spezielle Schulung von Datenschutzbeauftragten in Betracht, deren erfolgreicher Abschluss durch ein Zertifikat bestätigt werden könnte. Anforderungen an derartige Schulungen künftiger oder bereits benannter Datenschutzbeauftragter[996] könnten durch die Selbstverwaltungsorganisationen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden oder in der bereits erwähnten Rechtsverordnung festgeschrieben werden. Eine Zusammenarbeit mit Universitäten und Fachhochschulen wäre wünschenswert.

---

990 U.a. Zusammenfassung des Workshops am 14.3.2001, Anhang 4.3, S. 260 ff.

991 Wet bescherming persoonsgegevens vom 6.7.2000, Amtsblatt 302.

992 Forderungen des *BvD* zur 2. Phase der Novellierung des BDSG, Anhang 6, S. 281 ff.

993 S. z.B. *Bergmann/Möhrle/Herb*, § 36 Rn. 52; *Tinnefeld/Ehmann* 1998, 407f.; *LG Ulm*, DuD 1991, 154 ff.

994 S. Anhang 6, S. 288.

995 S. UGB-KOM-E 1998, 748.

996 Verschiedentlich existieren bereits Ausbildungsgänge.

Angesichts der sich ständig ändernden Anforderungen und Möglichkeiten der Datenverarbeitung und -technik sollte ein gesetzlich verbrieftes Recht auf Weiterbildungszeiten vorgesehen werden. Die Einzelheiten könnten ebenfalls in der oben genannten Rechtsverordnung geregelt werden.[997]

Gleichermaßen sollten Mindeststandards für die personelle und sachliche Ausstattung der betrieblichen und behördlichen Datenschutzbeauftragten geregelt werden.[998]

Schließlich sollte im Interesse einer effektiven Kontrolle – im übrigen auch im Hinblick auf die entfallende Meldepflicht nach § 4d Abs. 2 BDSG – eine Anzeigepflicht der Bestellung eines betrieblichen oder behördlichen Datenschutzbeauftragten gegenüber den Kontrollstellen vorgesehen werden. Die Anzeige sollte auch Aussagen über die Zuverlässigkeit und Fachkunde (z.B. der Nachweis einer entsprechenden Schulung) sowie die zeitliche, personelle und sachliche Ausstattung treffen.[999] Dadurch werden die Kontrollstellen in die Lage versetzt zu prüfen, ob sie von ihrem Recht, nach §38 Abs. 5 Satz 3 BDSG die Abberufung des Datenschutzbeauftragten zu verlangen, Gebrauch machen sollten.

Ein neues BDSG sollte auch die Funktion eines Konzerndatenschutzbeauftragten aufnehmen. Dies würde zu wünschenswerten Synergieeffekten führen und die Rolle des Datenschutzes im gesamten Konzernverbund stärken. Nicht die – häufig nebenamtlich tätigen – jeweiligen Datenschutzbeauftragten der einzelnen Tochterunternehmen würden für die Durchsetzung des Datenschutzes verantwortlich sein, sondern ein der Größe des Gesamtkonzerns entsprechend mit Personal und Sachmitteln ausgestatteter Konzerndatenschutzbeauftragter. Diese Datenschutz-„task forces“ hätten angesichts ihres erweiterten Wirkungskreises eine wesentlich herausgehobenere Stellung gegenüber den einzelnen Unternehmen eines Konzerns und in ihrer Tätigkeit ein größeres Gewicht. Für die Konzerne wären Fragen des Datenschutzes nicht mehr zersplittert durch die jeweiligen Tochterunternehmen zu regeln, sondern gebündelt durch eine Stelle. Einem vom deutschen Datenschutzrecht sanktionierten Konzerndatenschutzbeauftragten wird es darüber hinaus in weltweit tätigen Konzernen leichter fallen, Datenschutzgrundsätze im gesamten Konzern durchzusetzen.

Die bisherige Regelung von Kontrollbefugnissen des betrieblichen oder behördlichen Datenschutzbeauftragten gegenüber der Mitarbeitervertretung ist unbefriedigend. Sie führt - auch angesichts der begrenzten Kontrollmöglichkeiten öffentlicher Kontrollstellen (Aufsichtsbehörden) – faktisch zu einem weißen Fleck im Datenschutz. Ob Betriebs- oder Personalräte als Teil der „speichernden Stelle“ der Kontrolle der betrieblichen oder behördlichen Datenschutzbeauftragten bereits jetzt unterliegen, ist heftig umstritten.[1000] Das *BAG* verneint dies und spricht insoweit hinsichtlich des BDSG, das dieses Verhältnis nicht regelt, von einem lückenhaften Gesetz.[1001] Es stützt sich dabei insbesondere auf das Argument, dass die Kontrolltätigkeit des betrieblichen Datenschutzbeauftragten dem Arbeitgeber zuzurechnen sei, da der Datenschutzbeauftragte keine „neutrale Stellung“ zwischen Arbeitgeber und Betriebsrat einnehme. Eine Kontrolltätigkeit sei daher mit der Unabhängigkeit des Betriebsrats unvereinbar.

---

997 So auch der Entwurf eines § 156 Abs. 6 UGB: „Durch Rechtsverordnung können die Anforderungen an die Fachkunde und Zuverlässigkeit einschließlich der Weiterbildung der [...] zu bestellenden Umweltbeauftragten und deren Anzahl geregelt werden.“

998 Auf der Jahreskonferenz des Bundesverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. am 13.6.2001wurde die Bildung eines Arbeitskreises vereinbart, der entsprechenden Kriterien entwickeln soll.

999 S. § 156 Abs. 5 des Entwurfs eines UGB.

1000 *BAG*, RDV 1998, 64 (65) m.w.N.

1001 *BAG*, RDV 1998, 64 (66).

Die Lücke, die das BDSG nach Auffassung des *BAG* enthält, sollte geschlossen werden. Es ist nach Auffassung der Gutachter auch mit der Unabhängigkeit der Mitarbeitervertretung vereinbar, diese in die Kontrolltätigkeit einzubeziehen. Um bezogen auf diesen Bereich eine „neutrale Stellung" des betrieblichen Datenschutzbeauftragten zwischen Arbeitgeber und Betriebsrat zu unterstreichen, käme eine Einbeziehung der Betriebs- und Personalräte in Form einer effektiven und echten Mitbestimmung bei der Bestellung der Datenschutzbeauftragten in Betracht.[1002] Die Unterstützungspflicht gemäß § 4f Abs. 5 BDSG könnte dann zur Klarstellung auch auf Betriebsräte erstreckt werden.[1003]

Die in der Begleitkommission und in den Fachgesprächen wiederholt eingeforderte Verabschiedung eines Arbeitnehmerdatenschutzgesetzes wird auch von den Gutachter dringend empfohlen.

9.3 Gesellschaftliche Kontrolle

Der Selbstregulierung durch gesellschaftliche Kräfte entspricht es, diese auch für Beiträge zu einer wirksamen Umsetzung des Datenschutzrechts zu gewinnen. Entsprechend der steigenden wirtschaftlichen Bedeutung der Datenverarbeitung nimmt auch die Bedeutung des Datenschutzes für den Wettbewerbs- und Verbraucherschutz zu. Daher sollte – über die interne und externe staatliche Kontrolle hinaus – auch eine gesellschaftliche Kontrolle der Einhaltung von Datenschutzvorschriften in der Form möglich sein, dass Wettbewerber und anerkannte Verbände[1004] die Unterlassung datenschutzrechtswidriger Praktiken geltend machen können.

9.3.1 Konkurrentenklagen

Durch Ergänzung des UWG ist klarzustellen, dass Wettbewerber den Verstoß gegen Datenschutzpflichten im Rahmen einer privatrechtlichen Konkurrentenklage als unlauteren Wettbewerbsvorteil geltend machen können. Hierzu ist klarzustellen, dass die Verletzung von gesetzlichen Datenschutzanforderungen und von anerkannten Verhaltensregeln einen Verstoß gegen die guten Sitten im Sinn des § 1 UWG und unzutreffende Datenschutzerklärungen eine irreführende Angabe in Sinn von § 3 UWG sein können. Dann kann jeder Wettbewerber den Wettbewerbsverstoß im Rahmen einer Unterlassungsklage geltend machen.

Bisher war umstritten, ob Datenschutzverstöße die beiden Generalklauseln der §§ 1 und 3 UWG erfüllen können.[1005] Durch diese Regelung wird klargestellt, dass ein Verstoß gegen Datenschutzrecht wettbewerbsrechtsrelevant sein kann. Damit bleibt die Aufgabe und Struktur des Wettbewerbsrechts erhalten. Die Datenschutzverstöße führen nicht durchgängig zu einer Sanktionierung nach Wettbewerbsrecht, sondern nur dann, wenn sie durch eine Handlung im geschäftlichen Verkehr begangen wurden. Eine solche Handlung setzt eine nach außen gerichtete Tätigkeit voraus, die irgendwie zur Förderung eines beliebigen Geschäftszwecks dient.[1006] Eine Unterlassungsklage nach §§ 1 oder 3 UWG ist also trotz eines Verstoßes gegen Datenschutzrecht nicht möglich, wenn dieser durch Handlungen im pri-

---

[1002] S. *Gola/Jaspers*, RDV 1998, 48.

[1003] S. *Gola/Jaspers*, RDV 1998, 48.

[1004] S. Teil 3 Kap. 6.3.

[1005] Ein Wettbewerbsverstoß im Sinn des § 1 UWG durch Rechtsbruch wird in der Regel nur angenommen, wenn die verletzten Normen wertbezogen sind und dem Schutz wichtiger Rechtsgüter und Interessen dienen. Dies wird für das Datenschutzrecht in der Rechtsprechung zum Teil angenommen – s. z.B. *BGH*, NJW 1992, 2419; *OLG Köln*, WRP 1982, 540; *OLG Koblenz*, DuD 1999, 358; *LG Mannheim*, NJW 1996, 1835; *LG Hamburg*, CR 1997, 21; *LG München I*, CR 1998, 83; *LG Stuttgart*, DuD 1999, 295; *OLG Köln*, RDV 2001, 103 ff. – zum Teil verneint – s. z.B. *OLG Frankfurt*, DuD 1997, 47 – und zum Teil offengelassen – s. z.B. *OLG Köln*, MMR 2000, 106, das letztlich aber doch den Wettbewerbsverstoß bejaht. s. aus der Literatur z.B. *Hoeren/Lütkemeier* 1999, 111f.; *Wuermeling*, CR 1996, 414f.; *v. Gamm*, GRUR 1996, 574 ff.

[1006] S. z.B. *Hoeren/Lütkemeier* 1999, 113.

vaten Bereich oder im internen Unternehmensbereich erfolgt. Die Klarstellung betrifft somit nur den Begriff der „guten Sitten“ im Rahmen des § 1 UWG und der „irreführenden Angaben“ im Rahmen des § 3 UWG.

Für diese Klarstellung erscheint eine Ergänzung des Satzes 2 von § 3 UWG nach dem Wort „Werbung“ um folgende Worte

„und Angaben über die Verarbeitung personenbezogener Daten.“

ausreichend. Sie stellt klar, dass ein Verstoß gegen Datenschutzvorschriften wettbewerbsrelevant sein kann. Diese Änderung des § 3 UWG wird auch die Auslegung der guten Sitten beeinflussen. Dass diese „Ausstrahlungswirkung“ gewollt ist, kann auch in der Begründung deutlich gemacht werden. Eine Änderung des klassischen Wortlauts des § 1 UWG erscheint daher für das Gewollte entbehrlich.

Neben einer privatrechtlichen sollte auch eine an § 13 UWG angelehnte öffentlich-rechtliche Konkurrentenklage möglich sein. Mit dieser sollen Wettbewerber die verwaltungsgerichtliche Überprüfung der Rechtmäßigkeit behördlicher Maßnahmen oder Unterlassungen beantragen können. Voraussetzung für die Klage ist, dass der Kläger geltend macht, dass die behördliche Maßnahme oder das behördliche Unterlassen geeignet ist, den Wettbewerb zu seinem Nachteil zu beeinträchtigen. Diese Beeinträchtigung muss dadurch erfolgen, dass der andere Wettbewerber gegen abschließend bestimmte datenschutzrechtliche Pflichten verstößt. Der Kläger muss zu dem anderen Gewerbetreibenden in einem Wettbewerbsverhältnis stehen, also Waren oder gewerbliche Leistungen gleicher oder verwandter Art für denselben Markt herstellen oder auf demselben Markt vertreiben. Eine Beeinträchtigung des Wettbewerbs kann zum Beispiel entstehen, wenn der Wettbewerber auf Grund der Missachtung datenschutzrechtlicher Pflichten – wie der Bestellung eines Datenschutzbeauftragten, unterlassener Unterrichtungen oder unterlassener Einholung von Einwilligungen – in der Lage ist, preiswerter anzubieten als der Kläger, der die datenschutzrechtlichen Pflichten erfüllt.[1007]

Die Möglichkeit der Konkurrentenklage könnte etwa durch folgende Regelung eröffnet werden:

Anbieter von Waren oder gewerblichen Dienstleistungen können die verwaltungsgerichtliche Überprüfung der Rechtmäßigkeit von behördlichen Maßnahmen oder Unterlassungen gegenüber anderen Anbietern beantragen, die Waren oder gewerbliche Leistungen gleicher oder verwandter Art auf demselben Markt anbieten. Die Klage ist nur zulässig, wenn der Kläger geltend macht, dass die behördliche Maßnahme oder das behördliche Unterlassen geeignet ist, den Wettbewerb zu seinem Nachteil zu beeinträchtigen, weil der andere Anbieter gegen abschließend bestimmte datenschutzrechtliche Vorschriften verstößt.

9.3.2 Verbandsklagen

Weiterhin sollen zur Unterbindung unlauteren Wettbewerbs durch datenschutzrechtswidrige Praktiken *anerkannte Verbände* Unterlassung geltend machen können. Hierzu ist § 13 Abs. 2 Nr. 3 UWG nach dem letzten Satz „Im Falle des § 1 können diese Einrichtungen den Anspruch auf Unterlassung nur geltend machen, soweit der Anspruch eine Handlung betrifft, durch die wesentliche Belange der Verbraucher berührt werden.“ um folgenden Satz zu ergänzen:

Dies gilt auch bei wesentlichen Verletzungen von Vorschriften zum Schutz der informationellen Selbstbestimmung.

[1007] S. zu dieser öffentlich-rechtlichen Konkurrentenklage den parallelen Vorschlag in § 46 des Entwurfs zu einem UGB und seine Begründung, UGB-Kom-E 1998, 540.

Zu weit vom Leitbild der gesetzlichen Regelungen abweichende Datenschutzklauseln in Allgemeinen Geschäftsbedingungen können heute schon nach § 13 AGBG als Verstoß gegen die Generalklausel des § 9 AGBG von anerkannten Verbraucherschutzverbänden durch Unterlassungsklage verhindert werden. Zur Kontrolle ausreichenden Datenschutzes in AGBs erscheint daher eine gesetzliche Ergänzung nicht erforderlich.

Nach § 22 AGBG kann derjenige von Verbraucherschutzverbänden auf Unterlassung verklagt werden, der – auch unabhängig von AGBs – „nicht nur im Einzelfall Vorschriften zuwiderhandelt, die dem Schutz der Verbraucher dienen (Verbraucherschutzgesetze)". In Absatz 2 werden die Verbraucherschutzgesetze abschließend aufgezählt. Hier sollte unter 10. aufgenommen werden:

10. die Vorschriften des Bundesdatenschutzgesetzes oder sonstiger Datenschutzregelungen, soweit die von der Datenverarbeitung betroffenen Personen Verbraucher sind.

10. Übergangsregelungen

Eine Reihe neuer technisch-organisatorischer Anforderungen setzen spezifische Vorkehrungen, Umgestaltungen der Datenverarbeitungsprozesse und Neuentwicklungen oder Anpassungen von Techniksystemen voraus. Für diese Vorbereitungen ist ein ausreichender Zeitraum einzuräumen, in dem bestimmte Vorschriften des Gesetzes erst zu einem späteren Zeitpunkt in Kraft treten. Bis dahin gelten die bestehenden Regelungen fort.

Ein modernisiertes Datenschutzgesetz sollte nicht mehr subsidiär sein, sondern Grundsätze enthalten, die auch für alle bereichsspezifischen Regelungen gelten. Dies macht eine Anpassung der bereichsspezifischen Regelungen an die Grundsätze des Gesetzes erforderlich. Dabei soll in den jeweiligen Fachbereichen auch geprüft werden, ob Verschärfungen oder Erleichterungen gegenüber den Grundsätzen geboten sind und ob Ausnahmen, die explizit und unter Verweis auf die Abweichung von der Grundregel formuliert sein müssen, notwendig sind. Hierfür muss eine angemessene Frist eingeräumt werden. Nach Ablauf dieser Frist gehen die Regelungen des BDSG den bereichsspezifischen Regelungen vor, wenn sie keine explizite Abweichung hiervon regeln.[1008]

In vielen Fällen müssen – insbesondere im nicht öffentlichen Bereich – die Datenverarbeitungsprozesse auf die neue Einwilligungslösung umgestellt werden. Diese kann für neu erhobene Daten ab dem Zeitpunkt des Inkrafttretens gelten. Für Daten, die bereits zuvor verarbeitet worden sind, könnte § 89 Abs. 7 Satz 2 TKG ein Vorbild sein. Danach dürfen vor Inkrafttreten des Gesetzes bereits erhobene Daten für die bis dahin zulässigen Zwecke weiterverarbeitet werden, wenn die betroffene Person hiergegen keinen Einwand erhebt. Ihre Einwilligung gilt als erteilt, wenn sie in angemessener Weise über ihr Einwandsrecht informiert worden ist und von ihrem Einwandsrecht keinen Gebrauch gemacht hat.

[1008] S. Teil 2 Kap. 3.1.

Literatur

Albers, M.: Zur Neukonzeption des grundrechtlichen „Daten“schutzes, in: *Kugelmann, A./Haratsch, D./Repkewitz, U.* (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, Stuttgart 1996, 113.

Albers, M.: Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001.

Arbeitskreis Datenschutz-Audit Multimedia: Prinzipien und Leitlinien zum Datenschutz bei Multimedia-Diensten, DuD 1999, 285.

Arbeitskreis „Datenschutzbeauftrage“ im Verband der Metallindustrie Baden-Württemberg (VMI): Datenschutz-Audit, DuD 1999, 281.

Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien, DuD 1997, 709.

Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Transparente Software – eine Voraussetzung für datenschutzfreundliche Technologien, www.datenschutz-berlin.de/doc/de/konf/57/hardsoft.htm oder www.bfd.bund.de/technik/aktech1.html.

Art. 29 – Datenschutzarbeitsgruppe: Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet, www.datenschutz-berlin.de/doc/eu/gruppe29/bbmem_de.htm;

Auernhammer, H.: Bundesdatenschutzgesetz, Kommentar, 3. Aufl. Köln u.a. 1993.

Baeriswyl, B.: Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, 6.

Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, DuD 1997, 446.

Bäumler, H.: Der neue Datenschutz, in: *Bäumler, H.* (Hrsg.), Der neue Datenschutz, Datenschutz in der Informationsgesellschaft, Neuwied 1998, 1.

Bäumler, H.: Datenschutzgesetzentwurf aus der Feder des Datenschutzbeauftragten, RDV 1999, 47.

Bäumler, H.: Das TDDSG aus Sicht eines Datenschutzbeauftragten, DuD 1999, 258.

Bäumler, H.: Modernisierung des Datenschutzes in Schleswig-Holstein. DuD 2000, 20.

Bäumler, H.: Datenschutzaudit und Gütesiegel in Schleswig-Holstein, DuD 2001, 252.

Bäumler, H./v. Mutius, A. (Hrsg.), Datenschutzgesetze der dritten Generation, Neuwied 1999.

Baudenbacher, C.: Kartellrechtliche und verfassungsrechtliche Aspekte gesetzesersetzender Vereinbarungen zwischen Staat und Wirtschaft - Ein Beitrag zu den staatlich inspirierten Selbstbeschränkungsabkommen, JZ 1988, 689.

Beckmann, M.: Produktverantwortung – Grundsätze und zulässige Reichweite, UPR 1996, 41.

Bergmann, L./Möhrle, R./Herb, A.: Datenschutzrecht: Handkommentar, 4 Bände, (Loseblattslg.) Stuttgart 1995 ff.

Bizer, J.: Forschungsfreiheit und informationelle Selbstbestimmung, Baden-Baden 1992.

Bizer, J.: Unabhängige Datenschutzkontrolle, DuD 1997, 481.

Bizer, J.: Zweckbindung durch Willenserklärung, DuD 1998, 552.

Bizer, J.: TK-Daten im Data Warehouse, DuD 1998, 570.

Bizer, J.: Kommentierung des TDDSG, in: *Roßnagel, A.* (Hrsg.), Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und zum Mediendienste-Staatsvertrag, Loseblatt, München 1999.

Bizer, J.: Datenschutz durch Technikgestaltung, in: *Bäumler, H.* (Hrsg.), Datenschutz der Dritten Generation, Neuwied 1999, 28.

Bizer, J.: Der Datentreuhänder, DuD 1999, 392.

Bizer, J.: Anonymität – Ein Rechtsprinzip der elektronischen Individualkommunikation, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000, 59.

Bizer, J.: Wozu Selbstregulierung in Deutschland?, DuD 2001, 126.

Bizer, J.: Gateway: Selbstregulierung des Datenschutzes, DuD 2001, 168.

Bizer, J.: Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 2001, 274.

Bizer, J.: Datenspeicherung in zentralen und peripheren Netzen versus SmartCards, in: *v. Zezschwitz, F./Möller, K. P.* (Hrsg.), Verwaltung im Zeitalter des Datenschutzes, 9. Wiesbadener Forum Datenschutz, Baden-Baden 2001, i.E.

Borking, J.: Der Identity Protector, DuD 1996, 654.

Borking, J.: Einsatz datenschutzfreundlicher Technologien in der Praxis, DuD 1998, 636.

Borking, J.: Privacy Incorporated Software Agent (PISA), DuD 2001, 411.

Breidenbach, R.: Outsourcing, in: *Bäumler, H./Breinlinger, A./Schrader, H.-H.* (Hrsg.), Datenschutz von A – Z, Neuwied 1999, O 400.

Breinlinger, A.: Datenschutzrechtliche Probleme bei Kunden- und Verbraucherbefragungen zu Marketingzwecken, RDV 1997, 247.

Breitfeld, A.: Berufsfreiheit und Eigentumsgarantie als Schranke des Rechts auf informationellen Selbstbestimmung, Berlin 1992.

Brohm, W.: Rechtsgrundsätze für normersetzende Absprachen - Zur Substitution von rechtverordnungen, Satzungen und Gesetzen durch kooperatives Verwaltungshandeln, DÖV 1992, 1025.

Brühann, U./Zerdick, T.: Umsetzung der EG-Datenschutzrichtlinie, CR 1996, 429.

Brühann, U.: Kommentierung des EG-Datenschutzrichtlinie, in: *Grabitz, E./Hilf, M.* (Hrsg.): Das Recht der Europäischen Union, Band 2, Sekundärrecht, Loseblatt München, A 30.

Bühnemann, B.: Datenschutz im nicht-öffentlichen Bereich, BB, Beilage 1/1974 zu Heft 3/1974, 1.

Büllesbach, A.: Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, RDV 1997, 239.

Büllesbach, A.: Das TDDSG aus Sicht der Wirtschaft, DuD 1999, 263.

Büllesbach, A.: Datenschutz in einem globalen Unternehmen, RDV 2000, 1.

Büllesbach, A.: Datenschutz in einem globalen Unternehmen, in: *Kubicek, H./Bracyk, H.-J./Klumpp, D./Roßnagel, A.* (Hrsg.), Global@Home, Jahrbuch Telekommunikation und Gesellschaft 2000, Heidelberg 2000, 282.

Büllesbach, A.: Datenschutz bei Data Warehouses und Data Mining, CR 2000, 11.

Büllesbach, A.: Konzeption und Funktion des Datenschutzbeauftragte vor dem Hintergrund der EG-Richtlinie und der Novellierung des BDSG, RDV 2001, 1.

Büllesbach, A./Garstka, H.: Systemdatenschutz und persönliche Verantwortung, in: *Müller, G./Pfitzmann, A.* (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn 1997, 383.

Büllesbach, A./Höss-Löw, P.: Vertragslösung, Safe Harbor oder Privacy Code of Conduct, DuD 2001, 135.

Büser, F.: Rechtliche Probleme im Rahmen der Datenübermittlung beim Franchising, BB 1997, 213.

Bull, H.-P.: Datenschutz oder die Angst vor dem Computer, München, 1984.

Bull, H.-P.: Mehr Datenschutz durch weniger Verrechtlichung – zur Überarbeitung von Form und Inhalt der Datenschutzvorschriften, in: *Bäumler H.* (Hrsg.), Der neue Datenschutz, Datenschutz in der Informationsgesellschaft, Neuwied 1998, 25.

Bull, H.-P.: Verfassungsrechtliche Vorgaben zum Datenschutz, Zur Entscheidung des Bayerischen Verfassungsgerichtshofs vom 11.11.1997, CR 1998, 385.

Bull, H.-P.: Neue Konzepte, neue Instrumente?, ZRP 1998, 310.

Bull, H.-P.: Aus aktuellem Anlaß: Bemerkungen über Stil und Technik der Datenschutzgesetzgebung, RDV 1999, 148.

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (Hrsg.), Umweltgesetzbuch (UGB-KomE), Entwurf der Unabhängigen Sachverständigenkommission zum Umweltgesetzbuch beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Berlin 1998.

Burchard, D., Verfassungsrechtliche Interessenabwägung im Informationsrecht, KritV 1999, 239.

BvD-Arbeitskreis: Die künftige Entwicklung des BDSG in Deutschland, DuD 2001, 271.

Caronni, G.: Anonymität - die Kehrseite der Medaille, DuD 1998, 633.

Cavoukian, A./Gurski, M./Mulligan, D./Schwartz, A.: P3P und Datenschutz, DuD 2000, 475.

Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM 24/2 (1981), 84.

Chaum, D.: Security without Identification: Transaction Systems to make Big Brother Obsolete, Communications of the ACM 28/10 (1985), 1030.

Clarke, R.: Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice, 1999, www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

Cranor, L. F.: Platform for Privacy Preferences – P3P, DuD 2000, 479.

Cranor, L. F.: Privacy Tools, in: *Bäumler, H.* (Hrsg.), E-Privacy – Datenschutz im Internet, Braunschweig 2000, 107.

Däubler, W.: Tarifvertragsrecht, 3.Aufl. Baden-Baden 1993.

Däubler, W./Klebe, T./Wedde, P.: Bundesdatenschutzgesetz, Köln 1996.

Dammann, U./Simitis, S.: EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997.

Degenhart, C.: Art. 5 GG, in: *Bieler, D.* (Hrsg.), Berliner-Kommentar zum Grundgesetz, Berlin 1997.

Demuth, T./Rieke, A.: Anonym im World Wide Web?, DuD 1998, 628.

Demuth, T./Rieke, A.: Der Rewebber – Anonymität in World Wide Web, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000, 38.

Dieckmann, U./Eitschberger, B./Eul, H./Schwarzhaupt, P./Wohlrab, G.: Datenschutzaudit – Quo Vadis?, DuD 2001, i.E.

Di Fabio, U.: Selbstverpflichtungen der Wirtschaft - Grenzgänger zwischen Freiheit und Zwang, in: *Kloepfer, M.* (Hrsg.), Selbst-Beherrschung im technischen und ökologischen Bereich: Selbststeuerung und Selbstregulierung in der Technikentwicklung und im Umweltschutz, Berlin 1998, 119.

Dix, A.: Das genetische Personenkennzeichen, DuD 1989, 235.

Dörr, E.: Die Folgen der Nichtbeachtung der Pflichten aus § 4 Abs. 2 BDSG, RDV 1992, 167.

Dörr, E./Schmid: Neues Bundesdatenschutzgesetz, 2. Aufl. Köln 1997.

Donos, P. K.: Datenschutz – Prinzipien und Ziele, Baden-Baden 1998.

Drews, H.-L.: Erneut: Zur Novellierung des Bundesdatenschutzgesetzes (BDSG), RDV 1987, 58.

Drews, H.-L./Kranz, H. J.: Argumente gegen die gesetzliche Regelung eines Datenschutz-Audits, DuD 1998, 98.

Drews, H.-L./Kranz, H. J.: Datenschutzaudit, DuD 2000, 226.

Drexl, J.: Die wirtschaftliche Selbstbestimmung des Verbrauchers, Tübingen 1998.

Duhr, E.: Datenschutz in Auskunfteien, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 7.5, i.E.

Duttge, G.: Recht auf Datenschutz. ein Beitrag zur Interpretation der grundrechtlichen Schutzbereiche, Der Staat 1997, 280.

Ehmann, H.: Informationsschutz und Informationsverkehr im Zivilrecht, AcP 188 (1988), 230.

Ehmann, H.: Neue Reformvorstellungen zum Datenschutzrecht, RDV 1989, 64.

Ehmann, H.: Prinzipien des deutschen Datenschutzrechts – unter Berücksichtigung der Datenschutz-Richtlinie der EG vom 24.10.1995 – (1. Teil), RDV 1998, 235, – (2. Teil), RDV 1999, 12.

Engel-Flechsig, S.: Einleitung zum TDDSG, in: *Roßnagel, A.* (Hrsg.), Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und zum Mediendienste-Staatsvertrag, Loseblatt, München 1999.

Engel-Flechsig, S./Maennel, F. A./Tettenborn, A.: Das neue Informations- und Kommunikationsdienste-Gesetz. NJW 1997, 2981.

Enquete-Kommission des Deutschen Bundestages „Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft“: Vierter Zwischenbericht zum Thema Sicherheit und Schutz im Netz, Juni 1998, BT-Drs. 13/11002.

Enzmann, M.: Introducing Privacy to the Internet User, DuD 2000, 535.

Ernestus, W.: Konzepte der Datensicherung, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 3.2, i.E.

Eul, H.: Datenschutz im Kreditwesen und im Zahlungsverkehr, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 7.2, i.E.

Federrath, H./Berthold, O.: Identitätsmanagement, in: *Bäumler, H.* (Hrsg.), E-Privacy – Datenschutz im Internet, Braunschweig 2000, 189.

Federrath, H./Pfitzmann, A.: „Neue" Anonymitätstechniken, DuD 1998, 623.

Federrath, H./Pfitzmann, A.: Bausteine zur Realisierung mehrseitiger Sicherheit, in: *Müller, G./Pfitzmann, A.* (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn 1997, 83.

Federrath, H./Pfitzmann, A.: Anonymität, Authentizität und Identifizierung im Internet, in: *Bartsch, M./Lutterbeck, B.* (Hrsg.), Neues Recht für neue Medien, Köln, 1998, 319.

Federrath, H./Pfitzmann, A.: Die Rolle der Datenschutzbeauftragte bei der Aushandlung von mehrseitiger Sicherheit, in: *Bäumler, H. (Hrsg.)*, Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 166.

Federrath, H./Pfitzmann, A.: Technische Grundlagen, in *Roßnagel* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 2.2, i.E.

Federrath, H./Pfitzmann, A.: Neues Datenschutzrecht und die Technik, in: *Kubicek u.a.* (Hrsg.), Internet@Future, Jahrbuch für Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 252.

Fiege, C.: Anonymer Zahlungsverkehr mit elektronischem Geld, CR 1998, 41.

Fisahn, A.: Ein Unveräußerliches Grundrecht am eigenen genetischen Code, ZPR 2001, 49

Fischer, K./Uthoff, R.: Das Recht der formularmäßigen Einwilligung des Privatpatienten bei externer Abrechnung, MedR 1996, 115.

Fox, D., Datenschutzbeauftragte als „Trusted Third Parties"?, in: *Bäumler, H. (Hrsg.)*, Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 81.

Gallwas, H.-U.: Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit, NJW 1992, 2785.

Gattung, G./Grimm, R./Pordesch, U./Schneider, M. J.: Persönliche Sicherheitsmanager in der virtuellen Welt, in: *Müller, G./Pfitzmann, A.* (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn 1997, 181.

Garstka, H.: Empfiehlt es sich, Notwendigkeit und Grenzen des Schutzes personenbezogener – auch grenzüberschreitender – Informationen neu zu bestimmen?, DVBl. 1998, 981.

Garstka, H.: Datenschutz in Netzen – Wandel der Technik und Grundzüge zukünftiger Regulierung, in: *Wiebe, A.* (Hrsg.), Regulierung in Datennetzen, Darmstadt 2000, 25.

Garstka, H.: Datenschutzkontrolle: Das Berliner Modell, DuD 2000, 289.

Geiger, A.: Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1989, 35.

Geis, I.: Individualrechte in der sich verändernde europäischen Datenschutzlandschaft, CR 1995, 171.

Gerling, R.: Datenschutzprobleme der Forschung, DuD 1999, 384.

Gerling, R.: Datenschutz in der Forschung, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 7.11, i.E.

Gesellschaft für Informatik: Stellungnahme zum Gesetzentwurf „Formvorschriften des Privatrechts", DuD 2001, 38.

Giesen, T.: Unabhängigkeit und Rechtskontrolle der Kontrollstellen nach Art. 28 der EG-Datenschutzrichtlinie, DuD 1997, 529.

Globig, K.: Zulässigkeit der Erhebung, Verarbeitung und Nutzung im öffentlichen Bereich, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 4.7, i.E.

Godt, C.: Haftung für ökologische Schäden, Berlin 1997.

Gola, P.: Die Entwicklung des Datenschutzrecht im Jahre 1996/97, NJW 1997, 3411.

Gola, P.: Die Entwicklung des Datenschutzrecht im Jahre 1997/98, NJW 1998, 3750.

Gola, P.: Die Entwicklung des Datenschutzrecht im Jahre 1998/99, NJW 1999, 3753.

Gola, P.: Die Entwicklung des Datenschutzrecht im Jahre 1999/2000, NJW 2000, 3749.

Gola, P.: Einwilligung nach BDSG und AGB-Gesetz, DSB 10/99, 7.

Gola, P.: Der auditierte Datenschutzbeauftragte – oder von der Kontrolle der Kontrolleure, RDV 2000, 93.

Gola, P.: Informationelle Selbstbestimmung in Form des Widerspruchsrechts, DuD 2001, 278.

Gola, P./Jaspers, A.: Von der Unabhängigkeit des betrieblichen Datenschutzbeauftragten – Erkenntnisse aus der Rechtsprechung für die BDSG-Novellierung, RDV 1998, 47.

Gola, P./Schomerus, R.: Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft, ZRP 2000, 183.

Gola, P./Wronka, G., Das Widerspruchsrecht gegenüber der Verarbeitung personenbezogener Daten zu Zwecken der Werbung, RdA 1996, 217.

Golembiewski, C.: Entbehrlichkeit einer richterlichen Anordnung der DANN-Analyse bei Einwilligung des Betroffenen?, NJW 2001, 1036.

Gress, S.: Datenschutzprojekt P3P, DuD 2001, 144.

Gridl, R.: Datenschutz in globalen Telekommunikationssystemen: Eine völker- und europarechtliche Analyse der vom internationalen Datenschutzrecht vorgegebenen Rahmenbedingungen, Baden-Baden, 1999.

Grimm, R.: User Control over Personal Web Data, ISSE‘99, Proceedings, Berlin 1999.

Grimm, R./Löhndorf, N./Roßnagel, A.: E-Commerce meets E-Privacy, in: *Bäumler* (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig 2000, 133.

Grimm, R./Löhndorf, N./Scholz, P.: Datenschutz in Telediensten (DASIT), DuD 1999, 272.

Grimm, R./Roßnagel, A.: Weltweiter Datenschutzstandard?, in*: Kubicek, H./Braczyk, H.-J./Klumpp, D./Roßnagel, A.* (Hrsg.), Global@Home, Jahrbuch Telekommunikation und Gesellschaft 2000, Heidelberg 2000a, 293.

Grimm, R./Roßnagel, A.: P3P and the Privacy Legislation in Germany: Can P3P Help to Protect Privacy Worldwide? (zus. m. R.) htttp://www.w3.org/P3P, June 2000.

Grimm, R./Roßnagel, A.: Datenschutz für das Internet in den USA, DuD 2000, 446.

Grimm, R./Roßnagel, A.: Can P3P Help to Protect Privacy Worldwide?, in: ACM (Ed.) Multimedia Security, Proceedings of the International Workshop, November 2000b, 157.

Groß, T.: Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatisierung der Post, JZ 1999, 326.

Gundermann, L.: E-Commerce trotz oder durch Datenschutz?, K&R 2000, 225.

Gusy, C.: Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang?, KritV 2000, 52.

Hamm, R.: Datenschutz und Strafrecht – Anonymität als Grenze für Strafverfolgung, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000, 90.

Hammer, V.: Die 2. Dimension der IT-Sicherheit, Braunschweig 1999.

Hammer, V./Pordesch, U./Roßnagel, A.: Betriebliche Telefon und ISDN-Anlagen rechtsgemäß gestaltet, Berlin 1993.

Hammer, V./Pordesch, U./Roßnagel, A./Schneider, M. J.: Vorlaufende Gestaltung von Telekooperationstechnik - am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235, St. Augustin 1994.

Hammerbacher, H.: Die zu fordernde "ausreichende" Anonymisierung von Datensätzen, DuD 1984, 181.

Hassemer, W.: Über die absehbare Zukunft des Datenschutzes, DuD 1996, 195.

Hassemer, W.: Private sind schneller, schlauer und billiger als der Staat – Der Datenschutz braucht deshalb ein neues Konzept, Frankfurter Rundschau-Dokumentation, 19.4.1999, 11.

Hassemer, W.: Wenn Menschen zu Lasten der Freiheit auf Sicherheit setzen – Über den Verlust der Privatheit und die Aufgabe des Staates, Frankfurter Rundschau-Dokumentation, 13.7.2001, 7.

Hauck, E.: Wirtschaftsgeheimnisse – Informationseigentum kraft richterlicher Rechtsbildung?, Berlin 1988.

Heil, H.: Datenschutz durch Selbstregulierung – Der europäische Ansatz, DuD 2001, 129.

Hesse, K.: Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl. Heidelberg 1995.

Heibey, W.: Datensicherung, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 4.5, i.E.

Hillenbrand-Beck, R./Gress, S.: Datengewinnung im Internet, DuD 2001, 389.

Hoeren, T./Lütkemeier, S.: Unlauterer Wettbewerb durch Datenschutzverstöße, in: *Sokol, B.* (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, 107.

Hoffmann-Riem, W.: Art. 5 GG, in: Alternativ-Kommentar zum Grundgesetz, 2. Aufl. 1989.

Hoffmann-Riem, W.: Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: *Krämer, L./Micklitz, H.-W./Tonner, K.* (Hrsg.), Recht und diffuse Interessen in der Europäischen Rechtsordnung, Baden-Baden 1997, 777.

Hoffmann-Riem, W.: Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in: *Bäumler, H.* (Hrsg.), Der neue Datenschutz, Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 11.

Hollmann, A.: Patientengeheimnis und medizinische Forschung, MedR 1992, 177.

Holznagel, B./Sonntag, M.: Rechtliche Anforderungen an Anonymisierungsdienste – Das beispiel des JANUS-Projektes der FernUniversität Hagen, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000, 72.

Huband, K.: Kanadas neues Datenschutzgesetz, DuD 2000, 461.

Hube, M.: Technikfolgenabschätzung: Der niedersächsische Weg, DuD 1999, 31.

Huhn, M., Pfitzmann, A.: Technische Randbedingungen jeder Kryptoregulierung, in: *Müller, G., Pfitzmann, A.* (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn 1997, 497.

Idecke-Lux, S.: Der Einsatz von Multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundes-Immissionsschutzgesetz, Baden-Baden 2000.

Jacob, J.: Die EG-Datenschutzrichtlinie aus der Sicht des BfD, RDV 1993, 11.

Jacob, J.: Perspektiven des neuen Datenschutzrechts, DuD 2000, 5.

Jandach, T.: Datenschutzmaßnahmen beim Outsourcing der Bürokommunikation, Technisch-organisatorische Anforderungen, DuD 2001, 224.

Japanische Expertenkommission zur Erarbeitung eines Gesetzentwurfs für ein allgemeines nationales Datenschutzgesetz: Outline of Fundamental Legislation for Personal Information Protection, Tokyo 2000.

Jekewitz, J.: Zielfestlegungen nach § 14 Abs.2 Abfallgesetz – ein Regelungsinstrument mit fraglichem Rechtscharakter, DÖV 1990, 51.

Jung, P.: Rechtsfragen der Online-Schiedsgerichtsbarkeit, K&R 1999, 63.

Karstedt-Meierrieks, A.: Selbstregulierung des Datenschutzes – Alibi oder Chance?, DuD 2001, 287.

Kessel, W.: Kooperation der Datenschutzbeauftragte mit Hard- und Softwareentwicklern, in: *Bäumler, H. (Hrsg.)*, Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 182

Kloepfer, M.: Datenschutz als Grundrecht: Verfassungsprobleme der Einführung eines Grundrechts auf Datenschutz, Königstein 1980.

Kloepfer, M.: Umweltschutz als Kartellprivileg?, JZ 1980, 781.

Kloepfer, M.: Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Gutachten B für den 62. DJT 1998, D 5.

Kloepfer, M.: Pressefreiheit statt Datenschutz? – Datenschutz statt Pressefreiheit?, AfP 2000, 511.

Klug, C.: Persönlichkeitsschutz beim Datentransfer in die USA – Die Safe-Harbor-Lösung, RDV 2000, 212.

Klug, C.: Die Vorabkontrolle – Eine neue Aufgabe für betriebliche und behördliche Datenschutzbeauftragte, RDV 2001, 12.

Koch, C.: Scoringsysteme in der Kreditwirtschaft, Einsatz unter datenschutzrechtlichen Aspekten, MMR 1998, 458.

Köhntopp, M.: Generisches Identitätsmanagement im Endgerät, in: *Grimm, R./Röhm, A.* (Hrsg.): Materialien zum GI-Workshop „Sicherheit und Electronic Commerce - WSSEC 2000“, 23.-24. März 2000a, Darmstadt, 1.

Köhntopp, M.: Identitätsmanagement – Anforderungen aus Nutzersicht, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000b, 43.

Köhntopp, M.: Privacy Enhancing Technologies, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 3.3, i.E.

Königshofen, T.: Die Umsetzung von TKG und TDSV durch Netzbetrieber, Service-Provider und Telekommunikationsanbieter, RDV 1997, 97.

Königshofen, T.: Prinzipien und Leitlinien zum Datenschutz-Audit bei Multimedia-Diensten, DuD 1999, 266.

Königshofen, T.: Chancen und Risiken eines gesetzlich geregelten Datenschutzaudits, DuD 2000, 357.

Königshofen, T.: Die Telekommunikations-Datenschutzverordnung – TDSV, DuD 2001, 85.

Kopp, F. O./Schenke, W.-R.: Kommentar zur Verwaltungsgerichtsordnung, 12. Auflage, München 2000.

Kothe, W.: Die rechtfertigende Einwilligung, AcP 85 (1985), 105.

Kranz, H.-L.: Kundendatenschutz und Selbstregulierung im Luftverkehr, DuD 2001, 161.

Kranz, H. J.: Datenschutz im Reise- und Tourismusgewerbe, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 7.4, i.E.

Krader, G.: Neuer europäischer Datenschutz im Internet? – der Entwurf der Europäischen Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation – eine kritische Analyse, RDV 2000, 251.

Krahmer, U.: Sozialdatenschutz nach SGB I und X, Köln 1996.

Krause, P.: Das Recht auf informationelle Selbstbestimmung - BVerfGE 65, 1, JuS 1984, 268.

Kruse, H. W.: Lehrbuch des Steuerrechts I, München 1991.

Kugelmann, A., Die informatorische Rechtsstellung des Bürgers: Grundlagen und verwaltungsrechtliche Grundstrukturen individueller Rechte auf Zugang zu Informationen der Verwaltung, Tübingen 2001.

Kuitenbrouwer, F.: Self-Regulation: Some Dutch Experiences, in: *U.S. Department of Commerce* (Ed.), Privacy and Self-Regulation in the Information Age, Washington 1997, www.ntia.doc.gov/reports/privacy/selfreg3.htm.

Kutscha, M.: Datenschutz durch Zweckbindung – ein Auslaufmodell?, ZRP 1999, 156.

Ladeur, K.-H.: Der Umwelthaftungsfonds" – ein Irrweg der Flexibilisierung des Umweltrechts?, VersR 1993, 257.

Ladeur, K.-H.: Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, Zur „objektiv-rechtlichen Dimension" des Datenschutzes, DuD 2000, 12.

Ladeur, K.-H.: Datenverarbeitung und Datenschutz bei neuartigen Programmführern in „virtuellen Videotheken", MMR 2000, 715.

Lamberg, P.: „Stillschweigende" Einwilligung in die Verarbeitung personenbezogener Daten, DÖV 1979, 894.

Lütkemeier, S.: EU-Datenschutz-Richtlinie – Umsetzung in nationales Recht, DuD 1995, 597.

Mallmann, O.: Zweigeteilter Datenschutz? Auswirkungen des Volkszählungsurteils auf die Privatwirtschaft, CR 1988, 93.

Mallmann, O.: Zum datenschutzrechtlichen Auskunftsanspruch des Betroffenen, GewArch. 2000, 354.

Marx, R.: Kommentar zum Asylverfahrensgesetz, 4. Auflage, Neuwied 1999.

Mattern, F.: Pervasive/Ubiquitous Computing, Informatik-Spektrum 2001, 145.

Mattern, F./Langheinrich, M.: Allgegenwärtigkeit des Computers, Datenschutz in einer Welt intelligenter Alltagsdinge, in. *Müller, G./Reichenbach, M.* (Hrsg.), Sicherheitskonzepte für das Internet, Berlin 2001, 7.

Maunz, T./Dürig, G.: Grundgesetz-Kommentar, Loseblatt, München.

Mayen, T.: Die Auswirkung der Europäischen Datenschutzrichtlinie auf die Forschung in Deutschland, NVwZ 1997, 446.

Merold, R. M.: The Necessary Elements of Self-Regulatory Privacy Regimes and the Role of Consumer Education in a Self-Regulatory Privacy Regime, in: *U.S. Department of Commerce* (Ed.), Privacy and Self-Regulation in the Information Age, Washington 1997, www.ntia.doc.gov/reports/privacy/selfreg4.htm.

Mitrou, E.: Die Entwicklung der institutionellen Kontrolle des Datenschutzes, Baden-Baden 1993.

Möncke, U.: Data Warehouse - eine Herausforderung für den Datenschutz?, DuD 1998, 561.

Möller, F.: Ungeschliffene Diamanten - Data-Warehouse, Data-Mining, Datenschutz, DANA 3/1998, 4.

Möller, F.: Gar nichts muss der Müller tun. Online-Marketing, Safe Harbour Principles und Strategien für den Datenschutz, DANA 3/2000, 15.

Müller, R.: Mitgestaltung bei internationalen Sicherheitsstandards, in: *Bäumler, H. (Hrsg.)*, Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 173

Müller, G./Pfitzmann, A. (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Band 1: Verfahren, Komponenten, Integration, Bonn 1997.

Müller, G./Stapf, K.-H.: Mehrseitige Sicherheit in der Kommunikationstechnik, Band 2: Erwartung, Akzeptanz, Nutzung, Bonn 1998.

Müller, G./Rannenberg, K.: Multilateral Security in Communication, Vol. 3: Technology, Infrastructure, Economy, Bonn 1999.

Müller, G. F./Wächter, M.: Zur Aufnahme einer verschuldensunabhängigen Schadensersatzregelung in das BDSG, DuD 1989, 240.

Murswiek, D.: Art. 2 GG, in: *Sachs, M.* (Hrsg.), Grungesetz-Kommentar, 2. Aufl. München 1999.

Oldiges, M.: Staatlich inspirierte Selbstbeschränkungsabkommen der Privatwirtschaft, WiR 1973, 1.

Opaschowski, H. W.: Datenschutz in der Gesellschaft, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 2.1, i.E.

Overkleeft-Verburg, M.: Datenschutz zwischen Regulierung und Selbstregulation. Erfahrungen aus den Niederlanden, in: *Alcatel SEL Stiftung* (Hrsg.), Rechtliche Gestaltung der Informationstechnik, Stuttgart 1996, 41.

Paefgen, T. C.: Adresshandel und Medienprivileg, CR 1994, 14.

Palandt-*Thomas*, H.: .§ 823 BGB, Bürgerliches Gesetzbuch, 60. Aufl. München 2001.

Perritt, H. H.: Regulatory Models for Protecting Privacy in the Internet, in: *U.S. Department of Commerce* (Ed.), Privacy and Self-Regulation in the Information Age, Washington 1997, www.ntia.doc.gov/reports/privacy/selfreg3.htm.

Petersen, S.: Grenzen des Verrechtlichungsgebotes im Datenschutz, Münster 2000.

Petri, T. B.: Vorrangiger Einsatz auditierter Produkte, DuD 2001, 150.

Petri, T. B.: Das Scoringverfahren der SCHUFA, DuD 2001, 290.

Pfitzmann, B./Waidner M./Pfitzmann, A.: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, CR 1987, 712, 796 und 898.

Pfitzmann, B./Waidner, M./Pfitzmann, A.: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, DuD 1990, 243 ff. und 305 ff.

Pfitzmann, A.: Datenschutz durch Technik, DuD 1999, 405.

Pfitzmann, A.: Möglichkeiten und Grenzen von Anonymität, in: *Sokol, B.* (Hrsg.), Datenschutz und Anonymität, Düsseldorf 2000, 9.

Pfitzmann, A.: Entwicklung der Informations- und Kommunikationstechnik, DuD 2001, 194.

Pitschas, R.: Informationelle Selbstbestimmung zwischen digitaler Ökonomie und Internet, DuD 1998, 139.

Pitschas, R.: Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Referat M für den 62. DJT 1998, M 9.

Podlech, A.: Verfassungsrechtliche Probleme öffentlicher Datenbanken, DÖV 1970, 473.

Podlech, A.: Verfassungsrechtliche Probleme öffentlicher Informationssysteme, DVR 1972/73, 149.

Podlech, A.: Aufgaben und Problematik des Datenschutzes, DVR 1976, 23.

Podlech, A.: Individualdatenschutz – Systemdatenschutz, in: *Brückner, K./Dalichau, G.* (Hrsg.), Festgabe für Grüner, Percha 1982, 451.

Podlech, A.: Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik, Leviathan 1984, 97.

Podlech, A.: Art. 2 GG, in: Alternativ-Kommentar zum Grundgesetz, 2. Aufl. 1989.

Podlech, A./Pfeifer, M.: Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, 139.

Pordesch, U.: Sekretär oder Aufpasser? Zur möglichen Rolle von Personal Digital Assistants in der Dienstleistungsgesellschaft, in: *Kubicek, H./Müller, G./Neumann, K. H./Raubold, E./Roßnagel, A.* (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1995, Heidelberg 1995, 167.

Pordesch, U.: Persönliches Sicherheitsmanagement, DuD 1999, 81.

Pordesch, U.: Sicherheitsmanagement, in: *Roßnagel, A./Haux, R./Herzog, W.* (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig 1999, 153.

Pordesch, U./Hammer, V./Roßnagel, A.: Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen, Braunschweig 1991.

Pordesch, U./Roßnagel, A.: Elektronische Signaturverfahren rechtsgemäß gestaltet, DuD 1994, 82.

Professoren-Entwurf eines Umweltgesetzbuchs *(Kloepfer, M./Rehbinder, E./Schmidt-Aßmann, E./Kunig, P.)*, Allgemeiner Teil, Berichte des Umweltbundesamtes 7/90, Berlin 1990.

provet, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gutachten für den BMBF, 1996 <http://www.provet.org/bib/mmge> oder <http://www.iid.de/iukdg/doku.html>.

provet/GMD: Die Simulationsstudie Rechtspflege, Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.

Püttmann, F.: Rechtliche Probleme der Marktforschung im Internet, K&R 2000, 492.

Rat für Forschung, Technologie und Innovation: Informationsgesellschaft - Chancen, Innovationen und Herausforderungen, Bonn 1995, www.technologierat.de/vdi/frames/report95.htm.

Registratiekamer/Information & Privacy Commissioner: Privacy-enhancing Technologies: The path to Anonymity, Amsterdam 1995.

Reidenberg, J.: Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review 76 (1998), 553.

Reidenberg, J.: Restoring Amricans' Privacy in Electronic Commerce. Electronic Commerce Symposium, Berkeley Technology Law Journal, 14 (1999), 778.*Rieß, J.*: Signaturgesetz – Der Markt ist unsicher, DuD 2000, 530.

Robbers, G.: Der Grundrechtsverzicht, JuS 1985, 925.

Roessler, T.: Anonymität im Internet, DuD 1998, 619.

Roßnagel, A.: Datenschutz bei Praxisübergabe, NJW 1989, 2303.

Roßnagel, A.: Die (tele-)kommunikative Selbstbestimmung, KJ 1990, 257.

Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung, Grundrisse einer Forschungsdisziplin, Baden-Baden 1993.

Roßnagel, A.: Kommentierungen, in: *Koch, H.-J./Scheuing, D.* (Hrsg.), Gemeinschaftskommentar zum Bundes-Immissionsschutzgesetz, (Loseblatt) Düsseldorf seit 1994.

Roßnagel, A.: Freiheit durch Systemgestaltung. Strategien des Grundrechtsschutzes in der Informationsgesellschaft, in: *Nickel, E./Roßnagel, A./Schlink, B.* (Hrsg.), Die Freiheit und die Macht - Wissenschaft im Ernstfall, Festschrift für Adalbert Podlech, Baden-Baden 1994, 227.
Roßnagel, A.: Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society", ZRP 1997, 26.

Roßnagel, A.: Das Signaturgesetz - kritische Bemerkungen zum Entwurf der Bundesregierung DuD 1997, 75.

Roßnagel, A.: Rechtliche Aspekte mobiler Kommunikation; in: *Roßnagel, A./Haux, R./Herzog, W.* (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig, 1998, 189.

Roßnagel, A. (Hrsg.): Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, Loseblatt München 1999.

Roßnagel, A.: Datenschutz in globalen Netzen. Das TDDSG – ein wichtiger erster Schritt, DuD 1999, 253.

Roßnagel, A.: Möglichkeiten für Transparenz und Öffentlichkeit im Verwaltungshandeln – unter besonderer Berücksichtigung des Internet als Instrument der Staatskommunikation, in: *Hoffmann-Riem, W./Schmidt-Aßmann, E.* (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000a, 257.

Roßnagel, A.: Regulierung und Selbstregulierung im Datenschutz, in: *Kubicek, H./Braczyk, H.-J./Klumpp, D./Roßnagel, A.* (Hrsg.), Global@Home, Jahrbuch Telekommunikation und Gesellschaft 2000, Heidelberg 2000b, 385.

Roßnagel, A.: Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung, Braunschweig 2000c.

Roßnagel, A.: Audits stärken Datenschutzbeauftragte, DuD 2000, 231.

Roßnagel, A.: Datenschutzaudit in Japan, DuD 2001, 154.

Roßnagel, A.: Das neue Recht elektronischer Signaturen, Neufassung des SigG und Änderung des BGB und der ZPO, NJW 2001, 1817.

Roßnagel, A.: Allianz von Medienrecht und Informationstechnik?, in: ders. (Hrsg.), Allianz von Medienrecht und Informationstechnik - Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001, 13.

Roßnagel, A./Bizer, J.: Multimediadienste und Datenschutz, Stuttgart 1995.

Roßnagel, A./Haux, R./Herzog, W. (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig 1998.

Roßnagel, A./Pfitzmann, A./Garstka, H., Modernisierung des Datenschutzes, DuD 2001, 253.

Roßnagel, A./Pordesch, U.: Elektronische Signaturverfahren rechtsgemäß gestaltet, DuD 1994, 82.

Roßnagel, A./Scholz, P.: Datenschutz in Japan – Rechtslage und Rechtsreform für den Electronic Commerce, DuD 2000, 454.

Roßnagel, A./Scholz, P.: Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Roßnagel, A./Schroeder, U. (Hrsg.): Multimedia in immissionsschutzrechtlichen Genehmigungsverfahren, Köln 1999.

Roßnagel, A./Wedde, P./Hammer, V./Pordesch, U.: Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechniken, Opladen 1990.

Rothe, J.: Einbehaltung privater Telefongesprächsgebühren im Gehaltsabzugsverfahren, :DuD 1996, 589.

Rüpke, G.: Perspektiven für ein europäisches Datenschutzrecht – Eine Betrachtung aus deutscher Sicht, EuZW 1993, 149.

Rüttgers, J.: Telekommunikation und Datenvernetzung – eine Herausforderung für Gesellschaft und Recht, CR 1996, 51.

Schaar, P.: Datenschutzfreier Raum Internet?, CR 1996, 170.

Schaar, P.: Kommentierung des TDDSG, in: *Roßnagel, A.* (Hrsg.), Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und zum Mediendienste-Staatsvertrag, Loseblatt, München 1999.

Schaar, P.: Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, DuD 2000, 275.

Schaar, P.: Persönlichkeitsprofile im Internet, DuD 2001, 383.

Schaffland, H.-J./Wiltfang, N.: Bundesdatenschutzgesetz, Kommentar, Loseblatt Berlin.

Schapper, C. H./Dauer, P.: Kartellrecht und Datenschutz. Das Spannungsverhältnis am Beispiel der SCHUFA, CR 1987, 497.

Schapper, C. H./Dauer, P.: Die Entwicklung der Datenaufsicht im nicht-öffentlichen Bereich (I), RDV 1987, 169.

Schaub, G.: Handbuch des Arbeitsrechts, 9. Aufl. München 2000.

Schaub, G.: Erfurter Kommentar zum Arbeitsrecht, München 1998.

Scherer, J.: Rechtsprobleme normersetzender „Absprachen„ zwischen Staat und Wirtschaft am Beispiel des Umweltrechts, DÖV 1991, 1.

Schild, H.-H.: Meldepflichten und Vorabkontrolle, DuD 2001, 282.

Schild, H.-H.: Dreigestirn des BDSG: Erheben, Verarbeiten und Nutzen (Zur Problematik unterschiedlicher begriffe im Datenschutzrecht), DuD 1997, 444.

Schild, H.-H.: Datenerhebung, -verarbeitung und -nutzung, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 4.3, i.E.

Schlink, B.: Das Recht auf informationelle Selbstbestimmung, DSt 1986, 233.

Schlink, B.: Das Recht auf informationelle Selbstbestimmung, Der Staat 25 (1986), 233.

Schlink, B.: Datenschutz und Amtshilfe, NVwZ 1986, 249.

Schmidt, W.: Die bedrohte Entscheidungsfreiheit, JZ 1994, 241.

Schmidt-Preuß, M.: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, VVDStRL 56 (1997), 162.

Schmitt Glaeser, W.: Schutz der Privatsphäre, Handbuch des Staatsrechts, Band VI, § 129, Heidelberg 1989, 41.

Schmitz, P.: TDDSG und das Recht auf informationelle Selbstbestimmung, München, 2000.

Schneider, M./Pordesch, U.: Identitätsmanagement, DuD 1998, 645.

Schoch, F.: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), 158.

Scholz, P.: Data-Warehouse, Data-Mining, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 9.2, i.E.

Schrader, H.-H.: Datenschutz in den Grundrechtskatalog. Verfassungsrechtliche Aspekte des Recht auf informationelle Selbstbestimmung, CR 1994, 427.

Schrader, H. H.: Selbstdatenschutz mit Wahlmöglichkeiten, DuD 1998, 128.

Schrader, H. H.: Selbstdatenschutz: Effektive Wahrnehmung des Selbstbestimmungsrechts, in: *Bäumler, H. (Hrsg.),* Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 206.

Schrader, H.-H.: Einwilligung, in: *Bäumler, H./Breinlinger, A./Schrader, H.-H.* (Hrsg.), Datenschutz von A – Z, Neuwied 1999 ff.

Schulz, W.: Rechtsfragen des Datenschutzes bei Online-Kommunikation, LfR-Materialien, Band 23, Düsseldorf 1998.

Schulz, W.: Verfassungsrechtlicher „Datenschutzauftrag“ in der Informationsgesellschaft, Die Verwaltung 1999, 137.

Schulz, W./Korte, B.: Die offene Flanke der Medienprivilegien. Anmerkungen zur geplanten Novellierung des journalistischen Zeugnisverweigerungsrechts und des Datenschutzprivilegs, AfP 2000, 530.

Schulz, W./Korte, B.: Medienprivileg in der Informationsgesellschaft, KritV 2001, 113.

Schulze-Fielitz, H.: Art. 5, in: *Dreier, H.* (Hrsg.), Grundgesetz-Kommentar, Band 1, Tübingen 1996.

Schwartz, P.: Privacy ans Democracy in Cyberspace, Vanderbilt Law Review 52 (1999), 1611.

Simitis, S.: Datenschutz: Voraussetzung oder Ende der Kommunikation?, Festschrift für Coing, Band II, München 1982, 495.

Simitis, S.: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398.

Simitis, S.: Anmerkung zu BGH, JZ 1986, 186, JZ 1986, 188.

Simitis, S.: Programmierter Gedächtnisverlust oder reflektiertes Bewahren, in: *Fürst, W. u.a.* (Hrsg.), Festschrift für *W. Zeidler*, Bd. 2, Berlin 1987, 1475.

Simitis, S.: Lob der Unvollständigkeit – Zur Dialektik der Transparenz personenbezogener Informationen, in: *Däubler-Gmelin, H. u.a.* (Hrsg.), Festschrift für *G. Mahrenholz*, Baden-Baden 1994, 573.

Simitis, S.: Allgemeine Aspekte des Schutzes genetischer Daten, in: Schweizerisches Institut für Rechtsvergleichung (Hrsg.), Genanalyse und Persönlichkeitsschutz, Zürich 1994, 107.

Simitis, S.: „Sensitive Daten"- Zur Geschichte und Wirkung einer Fiktion, in: *Brem, E. u.a.*, (Hrsg.), Festschrift für *M. M. Pedrazinni*, Bern 1990, 46.

Simitis, S.: Privatisierung und Datenschutz, DuD 1995, 648.

Simitis, S.: Virtuelle Präsenz und Spurenlosigkeit, in: *Hassemer, W./Möller, K. P.* (Hrsg.), 25 Jahre Datenschutz, Baden-Baden 1996, 28.

Simitis, S.: Internet oder der entzauberte Mythos vom „freien Markt der Meinungen", in: *Assmann, H.-D.* (Hrsg.), Wirtschafts- und Medienrecht in der offenen Demokratie: Freundesgabe für *F. Kübler*, Heidelberg 1997, 285.

Simitis, S.: Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, 281.

Simitis, S.: Datenschutz - Rückschritt oder Neubeginn, NJW 1998, 2473.

Simitis, S.: Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, 714.

Simitis, S./Dammann, U./Geiger, H./Mallmann, O./Walz, S.: Kommentar zum Bundesdatenschutzgesetz, 4. Aufl. Baden-Baden 1994 ff.

Starck, C.: Art. 5 GG, in: *v. Mangoldt, H./Klein, F./Starck, C.* (Hrsg.), Kommentar zum Grundgesetz, Band 1, 4. Aufl. München 1999.

Steinmüller, W.: Das Volkszählungsurteil des Bundesverfassungsgerichts, DuD 2/1984, 91

Steinmüller, W.: Informationstechnologie und Gesellschaft, Darmstadt 1993.

Stern, K.: Das Staatsrecht der Bundesrepublik Deutschland, Band III/2, München 1994.

Steinmüller, W. u.a.: Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT-Drs. VI/3826.

Swire, P. P.: Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in: *U.S. Department of Commerce* (Ed.), Privacy and Self-Regulation in the Information Age, Washington 1997, www.ntia.doc.gov/reports/privacy/selfreg1.htm.

Tauss, J./Kollbeck, J./Mönikes, J.: Einführung: Wege in die Informationsgesellschaft, in: *dies.* (Hrsg.), Deutschlands Weg in die Informationsgesellschaft, Baden.Baden 1996.

Tinnefeld, M.-T.: Freiheit der Forschung und europäischer Datenschutz, DuD 1999, 35.

Tinnefeld, M.-T./Ehmann, E.: Externe Datenschutzbeauftragte im öffentlichen Bereich. CR 1989, 637.

Tinnefeld, M.-T./Ehmann, E.: Einführung in das Datenschutzrecht, 3. Aufl. München 1998.

Tinnefeld, M.-T./Viethen, H.-P.: Arbeitnehmerdatenschutz und Internet-Ökonomie – Zu einem Gesetz über Information und Kommunikation im Arbeitsverhältnis, NZA 2000, 977.

Trute, H.-H.: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), 213.

Trute, H.-H.: Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, 822.

Trute, H.-H.: Verfassungsrechtliche Grundlagen, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 2.5, i.E.

Uckermann, E. v.: Einwilligung nach BDSG – ein Mißverständnis?, DuD 1979, 163.

U.S. Department of Commerce: Privacy and Selfregulation, Washington 1997, www.ntia.doc.gov/reports/privacy/selfreg1.htm.

U.S. Federal Trade Commission: Self-Regulation and Privacy Online, A Report to Congress, July 1999 – www.ftc.gov/opa/1999/9907/report1999.htm.

U.S. Federal Trade Commission: Fair Information Practices in the Electronic Marketplace, www.ftc.gov/reports/ privacy2000/.

U.S. Federal Trade Commission: Online Profiling: A Report to the Congress, June 2000, www.ftc.gov/os/2000/06/ onlineprofilingreportjune2000.pdf.

Vogelgesang, K.: Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Vogt, U./Tauss, J.: Entwurf für ein Eckwerte-Papier der SPD-Bundestagsfraktion „Modernes Datenschutzrecht für die (golbale) Wissens- und Informationsgesellschaft“, Bonn 1998.

Weber, M.: EG-Datenschutzrichtlinie – Konsequenzen für die deutsche Datenschutzgesetzgebung, CR 1995, 297.

Weichert, T.: Datenschutzrechtliche Anforderungen an Chipkarten, DuD 1997, 266.

Weichert, T., Datenschutzrechtliche Probleme beim Adressenhandel, WRP 1996, 522.

Weichert, T.: Anforderungen an das Datenschutzrecht für das Jahr 2000, DuD 1997, 712.

Weichert, T.: Datenschutzberatung – Hilfe zur Selbsthilfe, in: *Bäumler, H. (Hrsg.)*, Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 213.

Weichert, T.: Datenschutz, in: *Kilian, W./Heussen, B.* (Hrsg.), Computerrechts-Handbuch, München, Stand 1999, Kap. 130 – 138.

Weichert, T.: Datenschutz – ein zahnloser Tiger?, NStZ 1999, 490.

Weichert, T.: Der Entwurf eines Bundesdatenschutzgesetzes von Bündnis 90/Die Grünen, RDV 1999, 65.

Weichert, T.: Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, in: *Bäumler, H. (Hrsg.)*, E-Privacy – Datenschutz im Internet, Neuwied 2000, 158.

Weichert, T.: Datenschutz als Verbraucherschutz, DuD 2001, 264.

Weichert, T.: Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463.

Wengert, G./Widmann, A./Wengert, K.: Bankenfusionen und Datenschutz - Eine kritische Betrachtung der Fusionspraxis, NJW 2000, 1289 = RDV 2000, 47.

Wenning, R./Köhntopp, M.: P3P im europäischen Rahmen, DuD 2001, 139.

Wente, J.: Recht auf informationelle Selbstbestimmung und absolute Drittwirkung der Grundrechte, NJW 1984, 1446.

Westin, A.: Privacy on the Internet, Everyone a Privacy Protection Officer?, Berlin 1997, http://ig.es.tu-berlin.de/~dsb/informat/heft26/westin.htm.

Winkelmann, T.: Falschauskünfte von Auskunfteien: Zum Verhältnis von § 824 BGB zu § 32 Abs. 2 BDSG, MDR 1985, 718.

Wittig, P.: Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, 59.

Wolff, H.-J./Bachof, O./Stober, R., Verwaltungsrecht, Band 2, 6. Aufl. München 2000.

Wohlgemuth, H. H.: Datenschutzrecht für Arbeitnehmer, 2. Aufl. Neuwied 1993.

Wohlgemuth, H. H.: Auswirkungen der EG-Datenschutzrichtlinie auf den Arbeitnehmerdatenschutz, BB 1996, 690.

Wuermeling, U.: Telefonbuch auf CD-ROM – urheberrechtliche, datenschutzrechtliche und wettbewerbsrechtliche Aspekte, CR 1996, 414.

v. Zezschwitz, F.: Konzept der normativen Zweckbegrenzung, in: *Roßnagel, A.* (Hrsg.), Handbuch des Datenschutzrechts, München 2001, Kap. 3.1, i.E.

Zöllner, W.: Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, 3.

Zuck, R.: Der totale Rechtsstaat, NJW 1999, 1517.

Anhang

1. Entwicklung der Informations- und Kommunikationstechnik[1009]

Einleitung

Möchte man die Entwicklung der Informations- und Kommunikationstechnik einschätzen, um gesetzgeberisch darauf angemessen zu reagieren, dann ist vor allem die zu erwartende (und ggf. zu beeinflussende) Entwicklung innerhalb der nächsten zehn Jahre relevant. Prognosen sind naturgemäß unsicher – insbesondere, wenn sie die Zukunft betreffen (Winston Churchill). Deswegen ist es sinnvoll, zurück auf eine Prognose zu schauen, die vor zehn Jahren gestellt wurde:

Andreas Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14/12 (1990) 620-627.

Nahezu alles dort Vorausgesagte ist eingetroffen bzw. gilt noch heute. Der Stand von 1990 bzw. 2000 sowie die Prognose für 2010 wird im Folgenden zusammengefasst.

Kurzfassung

Für (mindestens) die nächsten zehn Jahre ist mit sehr großer Prognosesicherheit weiterhin mit einer exponentiellen Steigerung der Leistungsentwicklung der Informations- und Kommunikationstechnik zu rechnen.

Konkret bedeutet dies

- eine Verhundertfachung der Rechenleistung,
- eine, je nach Speichermedium, Verzehn- bis Verzweihundertfachung der Speicherkapazität sowie
- mindestens eine Verzehnfachung der jedem Nutzer zur Verfügung gestellten Kommunikationskapazität der Weitverkehrsnetze

innerhalb eines Jahrzehnts.

Mobile Datenkommunikation, die im Jahre 1990 schwierig, aber bereits im Jahre 2000 problemlos möglich war, wird im Jahre 2010 selbstverständlich sein. Details sind in den folgenden Abschnitten zu finden.

Prognosen für die systemische Entwicklung, d.h. welche Systeme aus den zur Verfügung stehenden informations- und kommunikationstechnischen Komponenten gebaut und wie benutzt werden, sind naturgemäß weniger genau.

Persönliche Rechner (PCs) waren im Jahre 1990 unvernetzt (stand alone) oder lokal vernetzt, aber bereits im Jahre 2000 global vernetzt. Ihre Funktionalität und die in ihnen gespeicherten persönlichen Daten werden ganz oder teilweise in vielerlei vernetzte Geräte integriert werden: persönliche digitale Assistenten (PDAs), Mobiltelefone, Spielekonsolen, Set-Top-Boxen für das digitale Fernsehen.

Für die Rechnerbenutzung bedeutet dies: Während die meisten Menschen im Jahre 1990 Rechner nur nach einer Schulung und im Jahre 2000 ab der Schule benutzt haben, werden wir alle im Jahre 2010 Rechner implizit ab der Geburt benutzen. Die Rechnerbenutzung wird also leichter, kinderleicht und schließlich unbewusst.

[1009] Teile hiervon erschienen in: DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 25/4 (2001) 194-195. Stand der Überarbeitung ist Juli 2001.

Leistungsentwicklung der Rechner

Die Leistungsentwicklung kleiner Rechner ist in drei Tabellen beschrieben, die die Situation in den Jahren 1990 und 2000 beschreiben und für das Jahr 2010 prognostizieren (Bild 1).

Die Angabe für die Verdopplungs-/Halbierungszeit von 1990 stammt aus der Prognose von 1990 für den Zeitraum 1990 bis 2000. Der Wert für die Verdopplungs-/Halbierungszeit von 2000 gibt die im Zeitraum 1990 bis 2000 tatsächlich eingetretenen Zeiten an, die der Prognose für 2010 zugrunde liegen.

1990	*PC*	*Taschen-computer*	*Verdopplungs-/ Halbierungszeit*
Befehlsbreite	32 bit	8 bit	5 Jahre
Befehle / s	10 000 000	1 000 000	2 Jahre
Speicherkapazität	8 MByte	1/8 MByte	1,5 Jahre
Zugriffszeit	0,000 000 08 s	0,000 000 3 s	3 Jahre
Cachekapazität	1/32 MByte	–	1,5 Jahre
Zugriffszeit	0,000 000 025 s	–	3 Jahre
Abmessungen	Schuhkarton	180•100•27 mm	
Preis	10 000 DM	500 DM	

2000	*PC*	*Taschen-computer*	*Verdopplungs-/ Halbierungszeit*
Befehlsbreite	64 bit	32 bit	8 Jahre
Befehle / s	1 000 000 000	50 000 000	1,5 Jahre
Speicherkapazität	512 MByte	16 MByte	1,5 Jahre
Zugriffszeit	0,000 000 005 s	0,000 000 05 s	2,5 Jahre
Cachekapazität	2 MByte	–	1,5 Jahre
Zugriffszeit	0,000 000 002 s	–	3 Jahre
Abmessungen	Schuhkarton	120•80•10 mm	
Preis	5 000 DM	1000 DM	

2010	*PC*	*Taschen-computer*	
Befehlsbreite	128 bit	64 bit	
Befehle / s	100 000 000 000	5 000 000 000	
Speicherkapazität	65 536 MByte	2 048 MByte	
Zugriffszeit	0,000 000 000 3 s	0,000 000 003 s	
Cachekapazität	256 MByte	–	
Zugriffszeit	0,000 000 000 2 s	–	
Abmessungen	Schuhkarton	120•80•10 mm	
Preis	5 000 DM	1000 DM	

Bild 1: Leistungsentwicklung kleiner Rechner

Leistungsentwicklung der Massenspeicher

Unter Massenspeichern versteht man diejenigen Speicher, die zur längerfristigen und preiswerten Aufbewahrung größerer Datenmengen geeignet sind. Hierbei reicht „längerfristig“ von einigen Sekunden bis zu vielen Jahrzehnten.

Bei Massenspeichern unterscheidet man, ob das eigentliche Speichermedium fest in das Schreib-/Lesegerät eingebaut ist oder ein Wechsel durch den Benutzer möglich und vorgesehen ist. Letzteres ermöglicht die Verwendung vieler „billiger“ Speichermedien mittels eines „teuren“ Schreib-/Lesegerätes und etwas physischer Arbeit, die ein Mensch oder ein Roboter zu verrichten hat.

Bild 2 gibt einen Überblick über die 1990 bzw. 2000 verfügbaren und die für das Jahr 2010 erwarteten Massenspeicher.

1990		*magnetische Festplatte*	*Diskette*	*optische Platte*	*Streamer*
Kapazität		600 MByte	1,4 MByte	600 MByte	2300 MByte
Zugriffszeit		0,02 s	0,1 s	0,08 s	20 s
Abmessungen	*Gerät*	Schuhkarton	Zigarrenkiste	Schuhkarton	Schuhkarton
	Speichermedium	(fest eingebaut)	90•94•3 mm	CD	Video-8
Preis	*Gerät*	6000 DM	200 DM	9000 DM	8000 DM
	Speichermedium	(fest eingebaut)	4 DM	900 DM	50 DM

2000		*magnetische Festplatte*	*Diskette*	*optische Platte*	*Streamer*
Kapazität		80000 MByte	100 MByte	800 MByte	24000 MByte
Zugriffszeit		0,009 s	0,05 s	0,08 s	20 s
Abmessungen	*Gerät*	Zigarrenkiste	Zigarrenkiste	Zigarrenkiste	Zigarrenkiste
	Speichermedium	(fest eingebaut)	90•94•3 mm	CD	DAT
Preis	*Gerät*	800 DM	100 DM	400 DM	2000 DM
	Speichermedium	(fest eingebaut)	20 DM	3 DM	50 DM

2010		*magnetische Festplatte*	*Diskette*	*optische Platte*	*Streamer*
Kapazität		10000000 MByte	1000 MByte	16000 MByte	240000 MByte
Zugriffszeit		0,005 s	0,03 s	0,02 s	20 s
Abmessungen	*Gerät*	Zigarrenkiste	Zigarrenkiste	Zigarrenkiste	Zigarrenkiste
	Speichermedium	(fest eingebaut)	90•94•3 mm	DVD	DAT
Preis	*Gerät*	200 DM	50 DM	200 DM	1000 DM
	Speichermedium	(fest eingebaut)	20 DM	3 DM	50 DM

Bild 2: Leistungsentwicklung kleiner Massenspeicher

Leistungsentwicklung der Kommunikationsnetze

Kommunikationsnetze unterscheiden sich darin, wie und wieviel Information sie übertragen können und wie sie Information vom Sender zum Empfänger übertragen.

Übertragung

Die Übertragung findet entweder leitungsgebunden oder nicht leitungsgebunden statt. Nur letzteres ermöglicht mobile Endgeräte. Unter anderem weil bei *digitaler Übertragung* (im Gegensatz zu analoger) ein Qualitätsverlust vollständig vermieden werden kann, werden seit einigen Jahren zunehmend digitale Übertragungssysteme eingesetzt.

Als Übertragungsleitungen dienen üblicherweise

- verdrillte Kupferkabel (twisted pair), z.B. „normale“ Telefonkabel, die bei ISDN seit 1988 für die Übertragung von 144 kbit/s (= 144 000 bit pro Sekunde)[1010] und seit 2000 unter dem Namen DSL für die Übertragung von 768 kbit/s genutzt werden,
- Koaxialkabel, die z.B. bei Kabelfernsehen für die analoge Übertragung von etwa 50 Fernsehkanälen, bei dem lokalen Netz (LAN) Ethernet für die Übertragung von 100 Mbit/s und in Weitverkehrsnetzen für bis zu 800 Mbit/s genutzt werden,
- Glasfasern, über die fast beliebig viel übertragen werden kann. Die nutzbare Bandbreite wird heutzutage durch die Sende- und Empfangselektronik auf etwa 40.000 Mbit/s begrenzt und bei gleichen Kosten etwa alle zwei Jahre verdoppelt.

Nicht leitungsgebundene Übertragung findet üblicherweise als

- (Erd-)Funk,
- Satellitenfunk

statt. Da bei Funk in jedem durch die Senderstärke und die frequenzabhängigen Ausbreitungseigenschaften definierten lokalen Bereich das Frequenzspektrum nur einmal zur Verfügung steht, ist die Gesamtbandbreite bei nicht leitungsgebundener Übertragung im Gegensatz zu leitungsgebundener stark beschränkt. Allerdings führt die Aufteilung in immer kleinere Funkzellen bei den sogenannten Zellularfunknetzen dazu, dass der gleiche Teil des Frequenzspektrums in jeder zweiten Zelle wieder neu genutzt werden kann. Auf diese Weise können bei geeigneter Infrastruktur (genügend viele und geeignet positionierte Sendemasten für Basisstationen) in zehn Jahren unvorstellbare Teilnehmerzahlen mit Kommunikationsdiensten versorgt werden. Konkret überschritt im Oktober 2000 erstmals in Deutschland die Zahl der Handys mit 40 Millionen die der ortsfesten Privatanschlüsse. Die zugrundeliegende GSM-Technik stellt den Teilnehmern seit der Einführung im Jahre 1993 jeweils einen Funkkanal zur Verfügung, der für Sprachkommunikation oder für Datenkommunikation mit 9,6 kbit/s genutzt werden kann. Seit dem Jahr 2001 ist eine Kanalbündelungstechnik verfügbar, die bei geringen Investitionen in die Infrastruktur und geeigneten Handys auf Teilnehmerseite Datenkommunikation mit bis zu ca. 40 kbit/s ermöglicht.

Frühestens ab dem Jahr 2002 wird die nächste Generation der Zellularfunknetze (UMTS) Datenkommunikation mit bis zu 2 Mbit/s pro Teilnehmer erlauben – dies allerdings nur für sehr wenige Teilnehmer pro Zellularfunkzelle gleichzeitig und vermutlich erst ab dem Jahre 2005 flächendeckend.

Parallel zu UMTS werden lokale Funknetze (Funk-LANs) aufgebaut, die auf Datenkommunikation optimiert sind und Mobilität zunächst nur in einem engen geographischen Bereich,

[1010] Diese 144 kbit/s werden in zwei Nutzkanäle zu je 64 kbit/s und einen Signalisierungskanal von 16 kbit/s aufgeteilt.

etwa einem Büro-, Hotel- oder Flughafengebäude unterstützen. In diesem engen geographischen Bereich bieten sie deutlich höhere Datenraten – wobei sich alle Nutzer diese Datenrate allerdings teilen müssen. Für Telefonie wäre dies desolat, für Datenkommunikation funktioniert es gut.

Bild 3 gibt einen Überblick:

Ortsfeste Kommunikation				
1990	ISDN:	64 kbit/s	Ethernet:	10 Mbit/s
2000	DSL:	768 kbit/s	Ethernet:	100 Mbit/s
2010	???:	8000 kbit/s	???:	1000 Mbit/s
Mobile Datenkommunikation				
1990	schwierig			
2000	GSM:	9,6 kbit/s	Funk-LANs:	10 Mbit/s
2010	UMTS:	100 kbit/s		100 Mbit/s

Bild 3: Leistungsentwicklung der Kommunikationsnetze

Vermittlung vs. Broadcast

Bisherige Kommunikationsnetze waren dienstespezifisch entworfen. Beispielsweise wurden Hörfunk- und Fernsehprogramme gleichzeitig und permanent an alle potentiellen Empfänger gesendet (Broadcast). Hierbei ist im Kommunikationsnetz nicht beobachtbar, ob und ggf. welche Programme von wem empfangen werden. Im Gegensatz zu dieser sogenannten Massenkommunikation wurde die sogenannte Individualkommunikation schon immer individuell vermittelt, z.B. Telefongespräche. Zukünftig werden Kommunikationsnetze möglichst universell, d.h. nicht dienstespezifisch, gestaltet werden. Um für diese universellen Kommunikationsnetze die vorhandenen Leitungen möglichst gut zu nutzen und insbesondere das Verlegen neuer Leitungen zu vermeiden, planen die Telekommunikationsanbieter, immer mehr Dienste zu vermitteln. Hierbei fallen prinzipiell eine Menge personenbezogener Daten an. Zudem wird die Vermittlung inzwischen von frei speicherprogrammierbaren Rechnern vorgenommen, so dass niemand mehr prüfen kann, welche Daten, z.B. durch ein universelles transitives Trojanisches Pferd, an wen weitergegeben werden. Zusätzlich wurden und werden Abhörschnittstellen flächendeckend eingebaut, deren Nutzung sich keinesfalls auf die sogenannten Bedarfsträger beschränken dürfte.

Entsprechendes gilt für Zellularfunk. Hier besteht nicht nur wie in jedem Funknetz das Problem, dass Sender gepeilt werden können, sondern die Teilnehmer werden bei Verlassen kleiner lokaler Bereiche im nächsten an- und dann im vorherigen abgemeldet. Der Durchmesser dieser sogenannten (Funk-)Zellen liegt zwischen einigen hundert Metern in Ballungsgebieten und vielen Kilometern im ländlichen Raum und wird fortlaufend verkleinert, um größere Zahlen von Teilnehmern versorgen zu können. Das An- und Abmelden der Teilnehmerstationen in den Zellularfunkzellen geschieht schon zu Zwecken der Erreichbarkeit, also selbst dann, wenn kein Dienst in Anspruch genommen wird und deshalb ansonsten eine Peilung unmöglich wäre. Dadurch kann man umfassende Bewegungsbilder der Bevölkerung erhalten.

Prognose

Die heute ortsfest mögliche Nutzung des Internet wird im Jahre 2010 zu vergleichbaren Kosten und mit vergleichbar leistungsfähigen Endgeräten mobil möglich sein. Es ist zu erwarten, dass dies von einem größeren Teil der Bevölkerung dann auch mobil und zumindest teilweise unbewusst genutzt wird. Zusätzlich werden ortsfeste Rechner und Anschlüsse bzgl. Rechen- und/oder Übertragungsleistung deutlich anspruchsvollere Dienste ermöglichen.

2. Datenschutzfördernde Techniken[1011]

Kurzfassung:

Datenschutzfördernde Techniken sind am besten im Kontext der mehrseitigen Sicherheit zu verstehen:

Zuerst wird das Konzept *mehrseitige Sicherheit* und ihr Potential eingeführt. Dann werden Schutzziele und ihre Wechselwirkungen beschrieben. Nachdem einige grundlegende Sachverhalte über Sicherheitstechniken dargelegt wurden, wird ein geordneter Überblick über Techniken für mehrseitige Sicherheit gegeben. Datenschutz hat insbesondere mit Vertraulichkeitseigenschaften in IT-Systemen zu tun, die bekanntlich besonders schwer zu überprüfen und damit den Betroffenen besonders schwer glaubhaft zu machen sind. Hier spielt das Konzept der mehrseitigen Sicherheit seine volle Stärke aus. Eine Bewertung der Reife und Effektivität der beschriebenen Techniken für mehrseitige Sicherheit zeigt, dass einige unmittelbar eingesetzt werden sollten, während andere noch einigen Forschungs- und Entwicklungsbedarf aufweisen. Eine Systematik für das Gebiet Datenschutz durch Technik beschließt diesen Anhang.

1. Einführung und Überblick

Mehrseitige Sicherheit bedeutet Sicherheit für alle Beteiligten, wobei jede(r) anderen nur minimal zu vertrauen braucht:

- Jede(r) hat individuelle Schutzziele.
- Jede(r) kann seine Schutzziele formulieren.
- Konflikte werden erkannt und Kompromisse werden ausgehandelt.
- Jede(r) kann seine/ihre Schutzziele im Rahmen des ausgehandelten Kompromisses durchsetzen.

Ähnlich wie die Aufklärung die Menschen von der Unterdrückung durch abergläubisches Denken und autoritäre politische Modelle befreit hat, hat die Technik für mehrseitige Sicherheit das Potenzial, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un-)Sicherheit zu befreien.

Zunächst wird eine umfangreiche Sammlung von Schutzzielen beschrieben, sowie ihre verstärkenden und schwächenden Wechselwirkungen.

Danach werden einige grundlegende Tatsachen über die Randbedingungen sicherer Informations- und Kommunikationstechnik allgemein, sowie für mehrseitig sichere Technik im Besonderen erläutert. Dies hilft zu verstehen, welche Techniken besonders hilfreich oder gar essentiell sind, um sichere Informations- und Kommunikationssysteme zu konstruieren, zu nutzen und zu unterhalten.

Einige dieser Techniken können von verschiedenen Beteiligten unilateral genutzt werden. Bei anderen ist eine bilaterale Kooperation notwendig, z.B. die Zusammenarbeit der beiden Kommunikationspartner. Wieder bei anderen ist eine trilaterale Kooperation nötig. Ein Beispiel sind rechtlich bindende digitale Signaturen, die nicht nur der Kooperation von zumindest zwei Kommunizierenden bedürfen, sondern weiterhin mindestens einer vertrauenswürdigen dritten Partei, die die öffentlichen Schlüssel zertifiziert. Bei anderen Techniken ist sogar die multilaterale Zusammenarbeit einer großen Zahl von unabhängigen Parteien notwendig. Wir

[1011] Abschnitt 6 ist eine leichte Überarbeitung von: Andreas Pfitzmann: Datenschutz durch Technik – Vorschlag für eine Systematik; DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 23/7 (1999) 405-408.

verwenden diese Unterscheidung, um einen kurzen strukturierten Überblick über die bekannten Techniken für mehrseitige Sicherheit zu geben (siehe auch [Pfit_00]).

Zusammenfassend wird eine Bewertung von Reife und Effektivität der verschiedenen beschriebenen Techniken für (mehrseitige) Sicherheit gegeben. Dies unterstreicht, welche Techniken sofort eingeführt werden sollten, um die Sicherheit und Datenschutzgerechtheit bestehender Systeme zu verbessern oder als Basis für neu zu errichtende. Es verdeutlicht auch, für welche Techniken erst noch weiterer erheblicher Forschungs- und Entwicklungsbedarf besteht.

Auf der Basis dieses Überblicks über Techniken für mehrseitige Sicherheit kann dann eine Systematik für das Gebiet Datenschutz durch Technik entwickelt und leicht verstanden werden.

2. Schutzziele und ihre verstärkenden und schwächenden Wechselwirkungen

Vor zwanzig Jahren wurde Sicherheit nahezu mit *Vertraulichkeit* gleichgesetzt, beispielsweise im Orange Book [DoDS_83]. Vor fünfzehn Jahren wurden *Integrität* der Information und *Verfügbarkeit* der Funktionalität hinzugefügt, beispielsweise von Voydock and Kent [VoKe_83] und in den europäischen Kriterien für Sicherheitsevaluationen [ITSEC_91]. Vor zehn Jahren wurde *Zurechenbarkeit* als viertes Schutzziel hinzugefügt, beispielsweise in den Kanadischen Kriterien [CTCPEC_92].

Außerhalb des Hauptstroms der staatlich dominierten Sicherheitsforschung wurden *Anonymität* und *Unbeobachtbarkeit* vor fünfzehn Jahren relevante Themen [Chau_85, PfWa_87], als der Fortschritt der Speichertechnologie soweit war, dass alle personenbezogenen Daten nahezu kostenlos unbegrenzt gespeichert werden konnten. In den vergangenen Jahren förderten Versuche mancher Regierungen, den Gebrauch der Kryptographie zu reglementieren, und das Bestreben der Musik- und Filmindustrie, Techniken zur Kontrolle des Kopierens und Verbreitens digitaler Inhalte zu entwickeln, ungemein die Entwicklung der Steganographie, d.h. der alten Kunst und entstehenden Wissenschaft, wie Information in anderen, unverfänglichen Daten versteckt werden kann (*Verdecktheit*). Mobilfunknetze, die es ermöglichen, Personen unabhängig davon, wo sie sich befinden und was sie gerade tun, zu erreichen, brachten das Schutzziel *Erreichbarkeit* ins Bewusstsein, d.h. die Kontrollmöglichkeit, wer wen unter welchen Umständen mittels welcher Medien und Kommunikationsdienste erreichen kann. Elektronischer Handel schärfte den Sinn für *Verbindlichkeit*, d.h. Teilnehmer müssen ihre rechtlichen Pflichten innerhalb einer vernünftigen Zeitspanne erfüllen.

Tabelle 1 gibt kurze Charakterisierungen der erwähnten Schutzziele.

Vertraulichkeit: Geheimhaltung von Daten w ährend der Übertragung. Niemand au ßer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.

Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand au ßer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.

Anonymit ät: Nutzer k önnen Ressourcen und Dienste benutzen, ohne ihre Identit ät zu offenbaren. Selbst der Kommunikationspartner erf ährt nicht die Identit ät.

Unbeobachtbarkeit: Nutzer k önnen Ressourcen und Dienste benutzen, ohne dass andere dies beobachten k önnen. Dritte k önnen weder das Senden noch den Erhalt von Nachrichten beobachten.

Integrität: Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empf änger erkannt.

Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

Verfügbarkeit: Nutzbarkeit von Diensten und Ressourcen, wenn gew ünscht.

Erreichbarkeit: Zu einer Ressource oder einem Nutzer kann Kontakt aufgenommen werden, wenn gew ünscht.

Verbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erf üllen.

Tabelle 1: Charakterisierungen der Schutzziele

Die Unterscheidung zwischen Inhalt und Umfeld der Kommunikation erweist sich als hilfreich, Ordnung in diese Sammlung von Schutzzielen zu bringen [WoPf_00], vgl. Abb. 1.

	Inhalte	Umfeld
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

Abb. 1: Eine geordnete Sammlung von Schutzzielen

Natürlich gibt es zwischen diesen Schutzzielen Wechselwirkungen. Sie werden in [WoPf_00, WoPf_00d] detailliert erklärt und in Abb. 2 dargestellt.

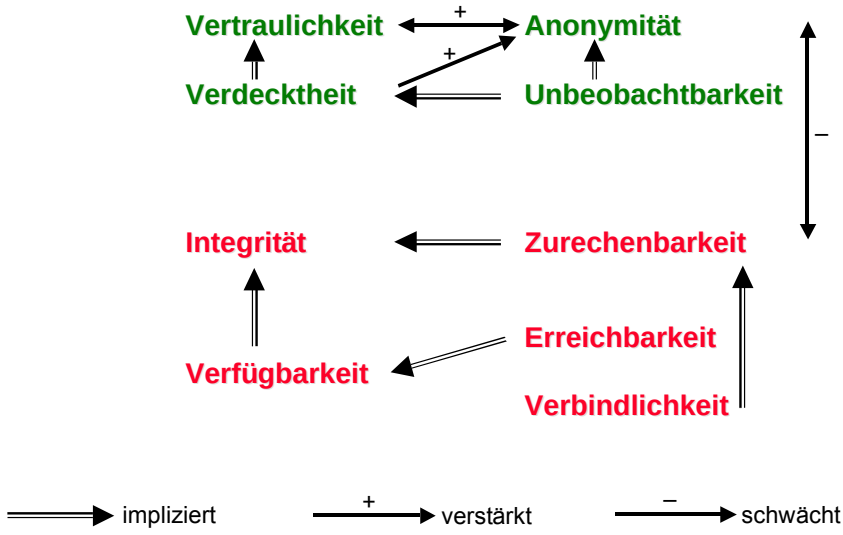


Abb. 2: Wechselwirkungen zwischen Schutzzielen

In der Zukunft werden sicherlich weitere Schutzziele definiert und wichtig werden.

3. Grundlegende Tatsachen

Wenn die Beteiligten, z.B. Benutzer, Dienstleister und Netzbetreiber, nicht bereit oder gar nicht in der Lage sind auszudrücken, welche Sicherheitseigenschaften sie erwarten, dann ist es unwahrscheinlich, dass sie bekommen, was sie wollen.

> —> Benutzer, Dienstleister und Netzbetreiber müssen bereit und in der Lage sein, alle Sicherheitseigenschaften zu formulieren, die sie erwarten.

Die von unterschiedlichen Beteiligten erwarteten Sicherheitseigenschaften sind üblicherweise sehr verschieden. Dies gilt nicht nur zwischen unterschiedlichen Anwendungen, sondern auch innerhalb derselben Anwendung. Zusätzlich können sich die Erwartungen im Zeitverlauf drastisch ändern, beispielsweise als Resultat negativer persönlicher Erfahrungen oder als Folge von Berichten in den Medien.

> —> Sicherheitseigenschaften müssen dynamisch anpassbar sein.

Die Sicherheit eines menschlichen Benutzers kann höchstens so gut sein wie die Sicherheit des Gerätes, mit dem er direkt interagiert.[1012] (Ob dieses Gerät für andere Beteiligte sicher ist, ist nur sekundär interessant.)

—> Geräte, die für ihre Benutzer sicher sind, sind nötig.

Wenn ein Gerät für die Integration von mehr als einer Anwendung vorgesehen ist, muss seine Sicherheit für die kritischste Anwendung ausreichen. Wird ein Gerät für allgemeine Anwendung gebaut, dann muss seine Sicherheit für die kritischste während seiner Gebrauchsdauer zu erwartenden Anwendung genügen. Ist dies nicht sichergestellt, dann ist das Gerät klarerweise nicht für allgemeine Anwendung geeignet – was beispielsweise für alle Rechner mit Windows 98/ME/CE oder Mac OS basierte PCs bis Version 9 einschließlich gilt.

—> Die Anforderungen an ein Gerät bzgl. Sicherheit werden durch die kritischste Anwendung bestimmt, für die das Gerät geeignet sein soll.

Sind die Entwerfer des Gerätes vorsichtig, werden die Anforderungen sogar durch die kritischste Anwendung bestimmt, für die das Gerät jemals benutzt werden wird – und diese Anwendung mag zu der Zeit, in der das Gerät entworfen wird, noch nicht einmal bekannt sein.

—> Geräte für menschliche Benutzer müssen eine sehr, sehr sichere Basis bilden, während ihrer Gebrauchsdauer weitere Sicherheitseigenschaften zu etablieren.

Das Löschen von Daten, die jemals in einem global vernetzten Informations- und Kommunikationssystem verfügbar waren, ist durch keine realistischen Maßnahmen zu erreichen. Zusätzlich verbilligt der technische Fortschritt Übertragung, Speicherung und Verarbeitung riesiger Datenmengen nahezu grenzenlos. Deshalb müssen, wo immer möglich, die Betroffenen in der Lage sein, bereits die Erfassungsmöglichkeit ihrer Daten zu verhindern.

—> Datenvermeidungs- und Datensparsamkeitstechniken beispielsweise durch Anonymität, Unbeobachtbarkeit und Unverkettbarkeit sind nötig. Wenn Zurechenbarkeit gefordert wird, sollte eine geeignete Form der Pseudonymität gewählt werden.[1013]

4. Überblick über Sicherheitstechniken

In diesem Abschnitt werden Sicherheitstechniken erwähnt und kurz erklärt. Er ist danach gegliedert, ob Sicherheitstechniken uni-, bi-, tri- oder nur multilateral anwendbar sind.

4.1 Unilateral nutzbare Techniken

Unilaterale Techniken können durch jede der Parteien selbst bestimmt werden. Es bedarf hierfür weder einer Koordination noch eines Aushandelns hinsichtlich ihrer Verwendung. Wichtige unilaterale Techniken für mehrseitige Sicherheit sind:

Werkzeuge, die selbst unerfahrenen Benutzern helfen, ihre Schutzziele zu formulieren, im Bedarfsfall für jede einzelne Anwendung oder jede einzelne Aktion [PSWW_98, WoPf_00]. Die Abbildungen 3 und 4 zeigen Beispiele.

[1012] Dies ist im Informations- und Kommunikationssystem sicherlich wahr. Außerhalb mag es Kompensation für Sicherheitsverletzungen geben. Aber dies kann natürlich bestenfalls für solche Schutzziele gelingen, für deren Verletzung Kompensation überhaupt möglich ist. Kompensation ist für Vertraulichkeitseigenschaften nicht möglich – Information, die öffentlich wurde, kann nicht mehr unöffentlich gemacht werden. Aber Kompensation ist für Integritäts- und Verfügbarkeitseigenschaften möglich, beispielsweise für Zurechenbarkeit und Verbindlichkeit, vgl. [Baum_99].

[1013] Eine strukturierte Erklärung, Definitionen von und Beziehungen zwischen Anonymität, Unbeobachtbarkeit, Unverkettbarkeit, Zurechenbarkeit und Pseudonymität ist in [WoPf_00, WoPf_00d, PfKö_01] zu finden.

Abb. 3: Benutzungsschnittstelle (Screenshot 1)

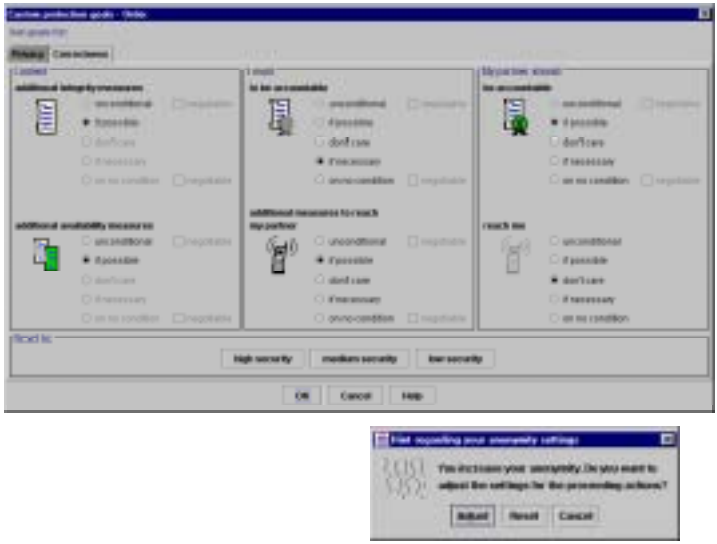


Abb. 4: Benutzungsschnittstelle (Screenshot 2)

(Portable) Geräte, die für ihre Benutzer sicher sind, als Basis jeder Datensicherheit. Die Geräte benötigen wenigstens ein Mindestmaß an physischem Schutz, der die direkte Ein- und Ausgabe für ihre Benutzer umfasst [PPSW_99], und im Fall von multifunktionalem Einsatz ein Betriebssystem mit feingestufter Zugriffskontrolle und mit einer Rechteverwaltung für verschiedene Anwendungen nach dem Prinzip der geringstmöglichen Privilegierung, vgl. Abb. 5. Diese ist essentiell, um die Verbreitung Trojanischer Pferde zu begrenzen. Sie kann die Verbreitung von Computerviren sogar vollständig verhindern.

Abb. 5: (Portable) Geräte, die für ihre Benutzer sicher sind, als Basis jeder Sicherheit

Verschlüsselung von lokalen Speichermedien, um die Inhalte vertraulich zu halten und/oder zu authentisieren.

Verstecken von geheimen Daten in lokalen multimedialen Inhalten oder in lokalen Dateisystemen [AnNS_98] unter Verwendung von Steganographie, mit dem Ziel, nicht nur den Inhalt der geheimen Daten zu schützen, sondern auch ihre Existenz geheimzuhalten.

Watermarking oder *Fingerprinting* digitaler Daten unter Nutzung steganographischer Techniken, um die Autorschaft oder Urheberrechtsverletzungen besser nachweisen zu können.

Ausschließliche Nutzung von *Software, deren Quellcode veröffentlicht und von vielen untersucht ist* oder *deren Sicherheit von vertrauenswürdigen unabhängigen Instanzen zertifiziert* ist, die Zugriff auf den vollständigen Quellcode und alle Werkzeuge zur Generierung des Objektcodes hatten. Am besten ist eine Kombination beider Ansätze hinsichtlich möglichst vieler der verwendeten Software-Bestandteile. Es bedarf zumindest des Einsatzes einer der beiden Ansätze, um einigermaßen sicher sein zu können, dass die verwendete Software keine trojanischen Pferde enthält. Das Gleiche gilt mehr oder weniger für *Hardware*, bei der alle Quellen und Werkzeuge, die bei der Gestaltung und der Produktion eingesetzt worden sind, auf das Nichtvorhandensein von trojanischen Pferden hin überprüft werden müssen.

4.2 Bilateral nutzbare Techniken

Bilaterale Techniken können nur genutzt werden, wenn die Kommunikationspartner zusammenarbeiten. Dies setzt für ihren Gebrauch eine gewisse Koordination und Absprache voraus. Wichtige bilaterale Techniken für mehrseitige Sicherheit sind:

Werkzeuge, um Schutzziele und Sicherheitsmechanismen bilateral *auszuhandeln,* vgl. [PSWW_98] und Abb. 6.

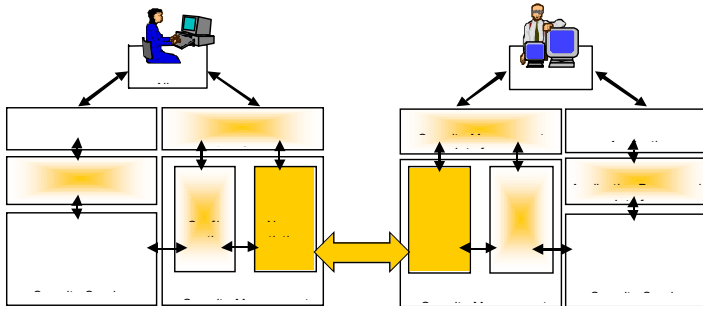


Abb. 6: Werkzeuge, um Schutzziele und Sicherheitsmechanismen bilateral auszuhandeln

Kryptographische und steganographische Mechanismen, um Kommunikationsinhalte zu schützen, siehe Abb. 7 und 8.

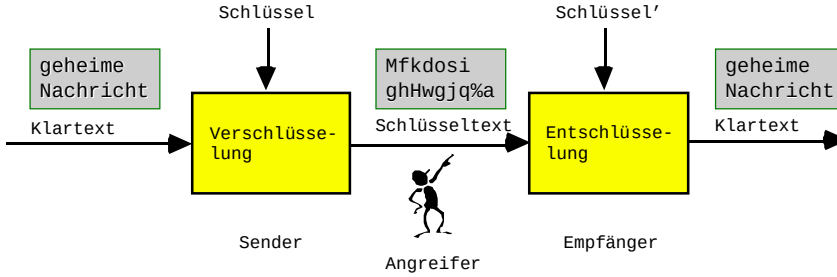


Abb. 7: Kryptographische Mechanismen, um Vertraulichkeit und Integrität der Kommunikationsinhalte zu schützen

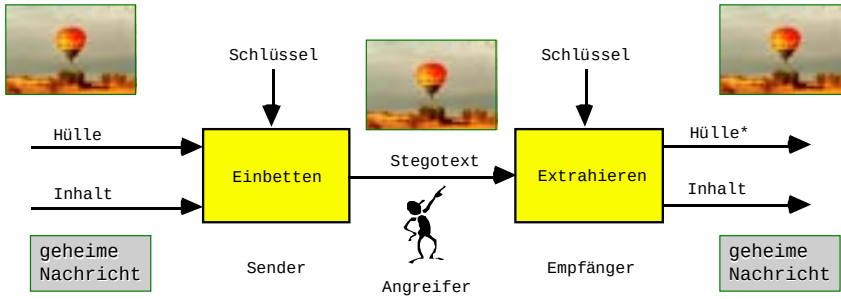


Abb. 8: Steganographische Mechanismen zum Verbergen der Existenz vertraulicher Kommunikationsinhalte

4.3 Trilateral nutzbare Techniken

Trilaterale Techniken setzen für ihre Nutzung eine dritte Partei voraus, die besondere Aufgaben für die anderen beteiligten Parteien erfüllt. Dies bedeutet, dass mehr Koordination und Aushandlung bei deren Nutzung notwendig ist im Vergleich zu den unilateralen und in der Regel auch den bilateralen Techniken. Wichtige trilaterale Techniken für mehrseitige Sicherheit sind:

Werkzeuge, um Sicherheitsmechanismen trilateral *auszuhandeln*, z.B. für Zurechenbarkeit.

Eine *Public-Key-Infrastruktur* (PKI), die Nutzern zertifizierte öffentliche Schlüssel anderer Nutzer zur Verfügung stellt, um deren digitale Signatur zu überprüfen und um den Nutzern die Möglichkeit zu geben, ihren eigenen öffentlichen Schlüssel zurückzuziehen, wenn der entsprechende private Schlüssel kompromittiert worden ist.

Sicherheitsgateways, um Inkompatibilitäten bzgl. Sicherheitsmechanismen oder Teilen von diesen zu überbrücken, vgl. Abb. 9. Sicherheitsgateways funktionieren gut in Bezug auf Mechanismen für Integrität und Zurechenbarkeit; sie sind aber nur von fragwürdigem Wert hinsichtlich Vertraulichkeit und Anonymität. Natürlich können Sicherheitsgateways keine Unvereinbarkeiten bzgl. Schutzzielen auflösen.

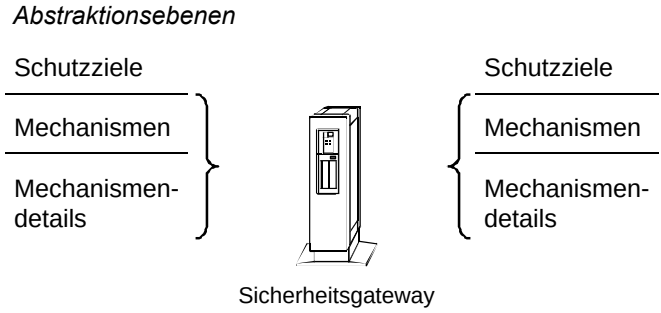


Abb. 9: Sicherheitsgateway zur Überbrückung inkompatibler Sicherheitsmechanismen

Mechanismen zur Schaffung von *digitalen Pseudonymen* als geeignete Kombination von Anonymität und Zurechenbarkeit [Chau_81]. Digitale Pseudonyme sind Testschlüssel digitaler Signatursysteme, die vollkommen anonym erzeugt und bei Bedarf mehr oder weniger anonym zertifiziert werden können. Insbesondere gibt es mit dem so genannten *Credential-Mechanismus* eine Möglichkeit, um sicher Signaturen (die für bestimmte Befugnisse stehen, sog. Beglaubigungen (Credentials)) zwischen verschiedenen Pseudonymen derselben Person zu transferieren [Chau_85, Chau_87, Chau_90, Chau_92].

Beim Einsatz von Pseudonymen für einen mehrseitig sicheren Werteaustausch gibt es verschiedene Möglichkeiten hinsichtlich der Aufgaben der einbezogenen dritten Partei [BüPf_90, PWP_90]:

- Identifikation des Nutzers im Betrugsfall (Pseudonyme sind zertifiziert und die Zertifizierungsstelle kennt die wirkliche Identität), d.h. der Pseudonymträger kann nicht überprüfen, ob sein Pseudonym aufgedeckt wurde und damit seine Anonymität nicht mehr gewährleistet ist.

- Geldhinterlegung bei einem aktiven Treuhänder zur Verhinderung von Betrug, wobei die Pseudonyme für die anderen Beteiligten völlig anonym bleiben, d.h. die Anonymität wird durch die Pseudonymträger selbst gesteuert.

4.4 Multilateral nutzbare Techniken

Multilaterale Techniken können nur zum Einsatz kommen, wenn eine größere Zahl unabhängiger Parteien zusammenwirken. Dies setzt in einem großen Maß Koordination und ggf. auch Aushandlung voraus. Wichtige multilaterale Techniken für mehrseitige Sicherheit sind:

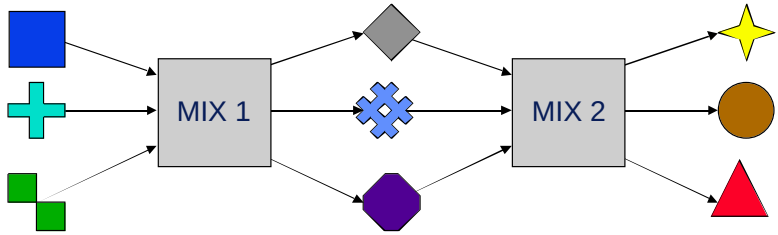
Werkzeuge, um multilateral Schutzziele und Sicherheitsmechanismen *auszuhandeln*, z.B. für Anonymität und Unbeobachtbarkeit.

Mechanismen, um *Anonymität, Unbeobachtbarkeit und Unverkettbarkeit* zu erreichen bei

- Kommunikation, d.h. zu schützen, wer wann von wo mit wem wohin kommuniziert [Chau_81, Chau_85, PfWa_87, CoBi_95, FeJP_96, JMPP_98, ReRu_99, GoRS_99], siehe Abb. 10,
- Zahlungen, d.h. zu schützen, wer wann an wen welchen Betrag für welche Leistung bezahlt [Chau_89, AJSW_97], und
- Werteaustausch, d.h. elektronisches Einkaufen vor Beobachtung zu schützen [BüPf_90, AsSW_97], siehe Abb. 11,

ohne Integrität, Verfügbarkeit oder Zurechenbarkeit zu kompromittieren.

In Abschnitt 6 werden diese Mechanismen in eine Systematik für das Gebiet Datenschutz durch Technik eingeordnet.



Funktionen jedes MIXes:

- Puffern
- Wiederholungen ignorieren
- Umcodieren
- Umsortieren

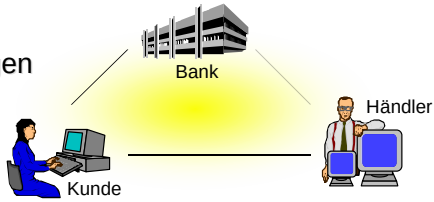
verbirgt so die Beziehung

Nachrichten

Abb. 10: Anonymität, Unbeobachtbarkeit und Unverkettbarkeit bei Kommunikation

digitale Signaturen relativ zu einem Pseudonym
Pseudonym = Public Key zum Testen digitaler Signaturen

Pseudonyme digitale Zahlungen



Werteaustausch zwischen pseudonymen Partnern

- œIdentifizierung bei Betrug (Pseudonyme sind zertifiziert und Zertifizierer kennt reale Identität): Anonymität ist durch Pseudonymträger nicht überprüfbar
- œ ä ändig anonymen Pseudonymen zu verhindern: Anonymität ist durch Pseudonymträger überprüfbar

Abb. 11: Pseudonyme digitale Zahlungen und Werteaustausch zwischen pseudonymen Parteien

5. Bewertung von Reifegrad und Wirksamkeit der Datensicherheitstechniken

Tabelle 2 stellt unsere Bewertung von Reifegrad und Wirksamkeit der in den vorigen Abschnitten beschriebenen Datensicherheitstechniken dar. Die Tabelle sollte von oben nach unten gelesen werden: Eine Datensicherheitstechnik in einer bestimmten Zeile ist Voraussetzung, bevor eine darunter aufgeführte Technik wirksam sein kann. In einigen Fällen werden Beispiele hinter dem Semikolon aufgeführt.

	Stand der öffentlichen Forschung	Demonstratoren und Prototypen	Verfügbare Produkte	Weit verbreitete Produkte
Physischer Schutz	kaum seriöse Publikationen	schwer zu beurteilen	schwer zu beurteilen; Me-Chip	sehr schlecht; Chipkarten
Sicherheitsevaluierung von IT	akzeptabel	schwer zu beurteilen	schwer zu beurteilen	schwer zu beurteilen
Sicherheit in Betriebssystemen	sehr gut	gut	schlecht; Windows NT, Windows 2000, Linux, Mac OS X	sehr schlecht; Windows 98, Windows ME, Windows CE, Mac OS 9
Kryptographie	sehr gut	gut	gut; PGP 2.6.x	akzeptabel; PGP 5.x, PGP 6.x
Steganographie	gut	akzeptabel	sehr schlecht	sehr schlecht
PKI	sehr gut	gut	schwer zu beurteilen	–
Sicherheitsgateways	gut	akzeptabel	–	–
Mechanismen für Anonymität, Unbeobachtbarkeit und Unverkettbarkeit	sehr gut	gut	akzeptabel; Onion Routing, Freedom, JAP	schlecht; Proxies
Digitale Pseudonyme	sehr gut	gut	gut; PGP 2.6.x	akzeptabel; PGP 5.x, PGP 6.x
Credential-Mechanismus	gut	–	–	–
Werkzeuge, die beim Formulieren und Verhandeln helfen	gut	akzeptabel	–	–
Integration dieser Techniken	akzeptabel	schlecht	schlecht	sehr schlecht

Tabelle 2: Reifegrad und Wirksamkeit von Datensicherheitstechniken

Man kann sehen, dass das schwächste Glied in der Sicherheitskette heute beim Endgerät der Nutzer liegt, insbesondere bei dessen physischem Schutz und dessen Betriebssystem. Um beides zu verbessern, muss noch viel getan werden.

Offensichtlich sind die Evaluierung von IT und die Integration von Datensicherheitstechniken diejenigen Herausforderungen für die Wissenschaft, die den größten Einfluss auf IT-Sicherheit haben.

6. Eine Systematik für das Gebiet Datenschutz durch Technik

In diesem Abschnitt wird eine Systematik des Gebietes „Datenschutz durch Technik“ entwickelt, in die die bekannten Datenschutzmaßnahmen eingeordnet werden.

6.1 Motivation

Eine Ordnung für Datenschutzmaßnahmen kann einerseits helfen, die Übersicht zu behalten oder wiederzugewinnen. Andererseits können die Ordnungskriterien vielleicht auch zur Bewertung von Datenschutzmaßnahmen dienen sowie ggf. zur Identifizierung von Lücken: Wo könnten weitere Datenschutzmaßnahmen erfunden und entwickelt werden? Welche Klassen von Datenschutzmaßnahmen werden in rechtlichen oder organisatorischen Regelungen nicht oder nur ungenügend beachtet?

6.2 Eine Ordnung der Datenschutzmaßnahmen

Für die Ordnung von Datenschutzmaßnahmen sind zwei Dimensionen hilfreich:

- Dient die Maßnahme eher der *Vertraulichkeit* von personenbezogenen Daten[1014] oder dient die Maßnahme vor allem der *Korrektheit*[1015] personenbezogener Daten (inkl. ihrer Aktualität)?
- Wie *stark* oder *schwach*, d. h. wie wirksam ist die Maßnahme in einem offenen Informations- und Kommunikationssystem? In einem offenen System kann jeder teilnehmen, so dass in ihm Maßnahmen der Personalauswahl und -schulung sowie der rechtlichen Regelung allenfalls begrenzt greifen.

Die folgende Abb. 12 ordnet die bekannten Datenschutzmaßnahmen nach diesen beiden Dimensionen, wobei Maßnahmen mit gleichem Ziel und ähnlicher Wirksamkeit zusammengefasst werden.

Die Vertraulichkeit von Daten ist dann am größten, wenn sie vollständig vermieden werden können – was natürlich nur bei nicht für eine bestimmte Zweckerfüllung benötigten Daten möglich ist. Dabei ist erstaunlich, wie viele einen Personenbezug herstellende Daten sich als unnötig herausstellen, wenn nur früh und gründlich genug nachgedacht und das Informations- und Kommunikationssystem entsprechend gestaltet wird. Beispielsweise ist es keineswegs erforderlich, dass der einen Telekommunikationsdienst Erbringende erfährt, welche Kommunikationspartner er miteinander verbindet. In der Maßnahmengruppe „unnötige Daten vermeiden“ (*Datenvermeidung*) lohnt es sich, zwischen Vermeiden der

- *Erfassungsmöglichkeit* (Schlagworte sind Unbeobachtbarkeit, Anonymität, Unverkettbarkeit [unbeobachtbare Kommunikation: Chau_81, Chau_88, Pfit_90, JMPP_98, Pfit_93, Fede_99; unbeobachtbare digitale Zahlungssysteme: Chau_85, Chau_89, Chau_92, BüPf_89, PWP_90]), der
- *Erfassung* [unbeobachtete Kommunikation, unbeobachtete Geldtransaktionen, etc.], der
- *Verarbeitung* und der
- *Speicherung*

zu unterscheiden. Die letzten beiden Punkte gehören zum Bereich der Anonymisierung.

Um die Korrektheit von Daten, die es nicht gibt, braucht man sich keine Sorgen zu machen: Diese Maßnahmengruppe ist und bleibt leer, vgl. Abb. 12.

[1014] Das Ziel des Datenschutzes *Vertraulichkeit personenbezogener Daten* entspricht einer möglichst weitgehenden Realisierung der Schutzziele *Vertraulichkeit*, *Anonymität* und *Unbeobachtbarkeit* aus Tabelle 1.

[1015] Das Ziel des Datenschutzes *Korrektheit personenbezogener Daten* entspricht den Schutzzielen *Integrität* und teilweise *Verfügbarkeit* aus Tabelle 1.

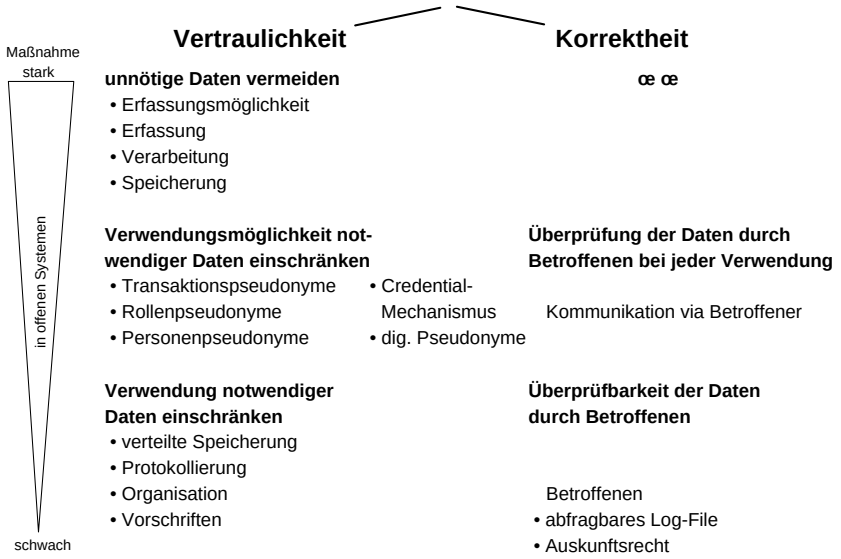


Abb. 12: Systematik der Datenschutzmaßnahmen

Kann man personenbezogene Daten nicht vermeiden, so ist das Zweitbeste, die Verwendungsmöglichkeit notwendiger Daten einzuschränken bzw. Betroffenen die Möglichkeit zu geben, die Daten insbesondere bei jeder Verwendung auf Richtigkeit und Aktualität zu überprüfen. Das Ziel der *Datensparsamkeit* umfasst, die Verwendungsmöglichkeit notwendiger Daten einzuschränken. Bei Betonung der informationellen Aspekte, d. h. welche Informationen worüber sind verfügbar, kann man konkretisierend von *informationeller Zweckbindung* sprechen, bei Betonung der Umsetzung durch technische Komponenten von *Zweckbindung durch Technik*.

Das wesentliche Hilfsmittel, die Verwendungsmöglichkeit notwendiger Daten einzuschränken, ist die Verwendung von *Pseudonymen* anstelle der üblichen Personenidentitäten [PWP_90, PfKö_01].

- *Transaktionspseudonyme* sind am wirksamsten, da sie jeweils nur für einen einzigen Vorgang verwendet werden, also außer durch den Pseudonyminhaber keinerlei Verkettung von verschiedenen Vorgängen ermöglichen, solange keine Möglichkeit zur Aufdeckung des Pseudonyms durch andere besteht.
- *Rollenpseudonyme* dienen zur Verkettung der Vorgänge innerhalb einer Rolle, z.B. in einer Geschäftsbeziehung. Sie werden für jede Rolle, in der sich der Nutzer befindet, unterschiedlich gewählt.
- *Personenpseudonyme* sind Personen zugeordnet und werden von ihnen in unterschiedlichen Rollen für die unterschiedlichsten Geschäftsbeziehungen und Transaktionen verwendet. Hierdurch ermöglichen Personenpseudonyme die Verkettung aller dieser Vorgänge und damit in der Regel bereits nach kurzer Zeit eine (Re-)Identifizierung des Pseudonymträgers.

Es sei hervorgehoben, dass zur Gewährleistung von Rechtssicherheit und Schadensvermeidung keineswegs eine Aufdeckbarkeit der Pseudonyme durch Dritte nötig ist, vgl. Abschnitt 4.3. Pseudonyme, die von Dritten nicht aufgedeckt werden können, bieten zweifellos stärkere Vertraulichkeit. Durch Dritte aufdeckbare Pseudonyme sind ein Beispiel für verteilte Speicherung und werden weiter unten eingeordnet.

Die stärkste Maßnahme, die Korrektheit von Daten sicherzustellen, ist die Überprüfung der Daten durch den Betroffenen bei jeder Verwendung. Ohne elektronische Vernetzung von Bürgerinnen und Bürgern, Verwaltungen und Firmen ist dies für viele Anwendungen zu aufwendig. Sobald der Betroffene einen für ihn sicheren persönlichen Rechner besitzt, online ist sowie alle vertraulichen Daten bei der Kommunikation sicher verschlüsselt werden und die Unverfälschtheit von Daten mittels digitaler Signaturen gesichert werden kann, kann alle Kommunikation von personenbezogenen Daten über den Betroffenen erfolgen. Er entscheidet, ob er dies will, um Richtigkeit, Aktualität, Relevanz und Vollständigkeit seiner Daten überprüfen zu können. Dies bedeutet nicht notwendigerweise, dass er immer als Mensch involviert ist, sondern er kann Routinevorgänge auch nach seinem Dafürhalten an seinen persönlichen Rechner delegieren. Der bereits heute gültige Grundsatz der Erhebung personenbezogener Daten vorzugsweise beim Betroffenen ist ein Spezialfall der gerade beschriebenen Maßnahme.

Hochinteressant ist, dass die Einschränkung der Verwendungsmöglichkeiten von Daten und die Überprüfung der Daten durch den Betroffenen bei jeder Verwendung trefflich kombiniert werden können (vgl. Abschnitt 4.3):

- Im einfachsten Fall erlauben dies *digitale Pseudonyme*.
- Besteht die Notwendigkeit, digital signierte Dokumente, die auf ein Transaktions- oder Rollenpseudonym ausgestellt sind, auf ein anderes Transaktions- oder Rollenpseudonym derselben natürlichen Person umzuformen, ermöglicht dies der *Credential-Mechanismus*.[1016]

Digitale Pseudonyme und der Credential-Mechanismus sind folglich zwischen den nur für Vertraulichkeit und den nur für Korrektheit arbeitenden Datenschutzmaßnahmen anzusiedeln, vgl. Abb. 12.

Die schwächsten dargestellten Maßnahmengruppen schränken die Verwendung notwendiger Daten ein bzw. stellen Überprüfbarkeit durch den Betroffenen her. Sie sind nicht notwendigerweise das Schlechteste: Gar nichts tun ist sicherlich schlimmer und selbst Überprüfbarkeit durch Stellvertreter (z. B. Datenschutzbeauftragte) ist schwächer, bürdet dem Betroffenen allerdings auch weniger Arbeit auf.

Die Verwendung notwendiger Daten einschränken (*Zweckbindung durch Organisation und Recht*) können

- *verteilte Speicherung*, d. h. mehrere speichernde Stellen müssen kooperieren, damit die jeweils vorliegenden Teile der Daten genutzt werden können (bei Verwendung von Kryptographie beispielsweise müssen Schlüsseltext und Schlüssel zusammengeführt werden, um zu entschlüsseln; oder nach einer Pseudonymisierung müssen die Stelle, die die pseudonymisierten Daten speichert, sowie die Stelle, die die Identifizierungsinformation zu den Pseudonymen verwaltet, zusammenarbeiten, um die Daten wieder personenbezogen verarbeiten zu können),

[1016] Dieses Verfahren ist natürlich viel datenschutzfördernder als der naive Ansatz, dem Empfänger des signierten Dokuments mitzuteilen oder gar zu beweisen, dass beide Pseudonyme derselben Person gehören. Denn wer wollte den Empfänger dieser Information hindern, sie auch in anderem Kontext zu verwenden?

- *Protokollierung*, d. h. es ist hinterher technisch feststellbar, wer welche Daten wozu verarbeitet hat,
- *Organisation*, d. h. Arbeitsorganisation inklusive Kontrolle, sowie
- *rechtliche Regelungen*, d. h. Verfassung, Gesetze, Verordnungen und Vereinbarungen.

Überprüfbarkeit der Daten durch Betroffene herstellen bzw. unterstützen können

- *mobile Datenverarbeitungssysteme*, d. h. die personenbezogenen Daten befinden sich auf Datenträgern im Besitz des Betroffenen, z. B. auf Chipkarten oder PDAs,
- *Mitteilungen an den Betroffenen bei jeder Verwendung* von Daten (auch dies ist nur dann generell praktizierbar, wenn der Betroffene via Netz erreichbar ist),
- durch den Betroffenen via Netz *abfragbares oder vor Ort einsehbares Log-File* (nur ersteres dürfte wirksam sein, wobei die Abfrage selbstverständlich verschlüsselt erfolgen sollte und auf Einträge zu begrenzen ist, die den Betroffenen betreffen), und – last and least – natürlich das ganz konventionelle
- *Auskunftsrecht*, das vielleicht via Netz häufiger in Anspruch genommen wird.

6.3 Diskussion der Systematik

Die Sortierung nach starken bzw. schwachen Maßnahmen in offenen Informations- und Kommunikationssystemen sagt naturgemäß wenig darüber aus, wie stark bzw. schwach die Maßnahme in einem geschlossenen, d. h. abgeschotteten, System ist. Beispielsweise können organisatorische Maßnahmen hochwirksam sein in Umgebungen, in denen Telekommunikation die Ausnahme ist, da die Rechner nicht vernetzt sind und mobile Datenträger (z. B. Disketten) kontrolliert werden. Allerdings dürfte dies, was vor zehn Jahren noch die Regel war, bereits heute, spätestens jedoch in zehn Jahren eine exotische Ausnahme sein.

Die daher grundsätzlich zu favorisierenden starken Maßnahmen der Datenvermeidung und Einschränkung der Datenverwendungsmöglichkeit erfordern, dass spätestens mit dem Betrieb des Informations- und Kommunikationssystems dessen Ziele abschließend klar sind. Dies sollte eigentlich für datenschutzrelevante Systeme eine Trivialität sein, dürfte aber in der Praxis wohl eher nicht der Fall sein. Dort mag durchaus das Bedürfnis bestehen (ob ihm nachgegeben werden sollte, ist eine andere Frage), erst einmal Daten zu sammeln, um dann später (ex post) zu entscheiden, ob und ggf. wie sie genutzt werden. Starke Maßnahmen sind in diesem Sinne *starr* (Entscheidung ex ante), schwache Maßnahmen *flexibel*.

Vielleicht noch eine einschränkende Bemerkung zur stärksten (und starrsten) Maßnahme: Ob die Erfassungsmöglichkeit unnötiger Daten vermieden wird, hängt u. a. von der Systemdefinition ab. Beispielsweise kann, etwa in ungewöhnlichen Situationen, auch eine Erfassung im Umfeld des Systems erfolgen. So ist etwa eine konventionelle Strafverfolgung selbst bei Anwendung dieser stärksten Maßnahme im informations- und kommunikationstechnischen System weiterhin möglich. Ein Beispiel ist die akustische Überwachung von Räumen, z. B. im Rahmen eines so genannten Großen Lauschangriffs. Damit können u. a. Telefongespräche unabhängig davon überwacht werden, wie sie innerhalb des Telekommunikationssystems geschützt werden.

Die Stärke bzw. Schwäche von Maßnahmen hängt davon ab, wem gegenüber ihre Wirkung betrachtet wird, d. h. sie ist vom zugrunde gelegten *Angreifermodell* abhängig. In der bisherigen Betrachtung wurden als Angreifer die Beteiligten, beispielsweise die Kommunikationspartner, angenommen und Alternativen, etwa Außenstehende, die die Kommunikation abhören, nicht diskutiert. Hier sei nur angedeutet, dass eine solche Betrachtung unterschiedlicher Angreifer erforderlich ist und zu einer Erweiterung der Ordnung der Datenschutzmaß-

nahmen führt: Statt einer Dimension für die Stärke bzw. Schwäche von Maßnahmen ist im schlimmsten Fall für jeden betrachteten Angreifer eine eigene Dimension nötig.

Dies sei am Beispiel Verschlüsselung erläutert: Zunächst wurde Verschlüsselung als Schutzmaßnahme vor Beteiligten betrachtet. Dabei kann es nur um den Schutz zu speichernder Daten gehen, wie oben erläutert wurde, und die Maßnahme ist unter „Verwendung notwendiger Daten einschränken; • verteilte Speicherung“ einzuordnen. Wird Verschlüsselung jedoch als Maßnahme gegen Außenstehende angewendet, dann vermeidet sie, dass die Außenstehenden die Nachrichteninhalte überhaupt erfassen können. Verschlüsselung ist dann unter „unnötige Daten vermeiden; • Erfassungsmöglichkeit“ einzuordnen.

7. Ausblick

Ein bewusst gestalteter, durch Werkzeuge technisch unterstützter Umgang mit den eigenen personenbezogenen Daten und die Verwendung von Anonymität oder anonymitätsnahen Pseudonymen (Transaktionspseudonymen, vgl. Abschnitt 6.2) wo immer möglich dürfte künftig unter dem vor wenigen Jahren hierfür geprägten Namen „*Identitätsmanagement*“ [ScPo_98, KöPf_01] eine große Bedeutung erlangen. Die beschriebenen Techniken der mehrseitigen Sicherheit bilden hierfür die notwendige Basis und die in Umfragen dokumentierte Unzufriedenheit der Nutzer mit den undurchschaubaren und bisher unkontrollierten Flüssen personenbezogener Daten im Internet die Motivation.

Literatur

[AJSW_97] N. Asokan, Phillipe A. Janson, Michael Steiner, Michael Waidner: The State of the Art in Electronic Payment Systems; Computer 30/9 (1997) 28-35.

[AnNS_98] Ross Anderson, Roger Needham, Adi Shamir: The Steganographic File System; Information Hiding, 2nd Workshop, Portland, Oregon, LNCS 1525, Springer, Heidelberg 1998, 73-82.

[AsSW_97] N. Asokan, Matthias Schunter, Michael Waidner: Optimistic Protocols for Fair Exchange; 4th ACM Conference on Computer and Communications Security, Zürich, April 1997, 6-17.

[Baum_99] Birgit Baum-Waidner: Ein Service zur Haftungsverteilung für kompromittierte digitale Signaturen; Verläßliche IT-Systeme, GI-Fachtagung VIS '99, DuD Fachbeiträge, Vieweg, Braunschweig 1999, 203-223.

[BüPf_89] Holger Bürk, Andreas Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

[BüPf_90] Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

[Chau_81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

[Chau_85] David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

[Chau_87] David Chaum: Sicherheit ohne Identifizierung; Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262-277; Datenschutz und Datensicherung DuD 12/1 (1988) 26-41.

[Chau_88] David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

[Chau_89] David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conference; Laxenburg (Austria), 1987, North-Holland, Amsterdam 1989, 69-93.

[Chau_90] David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, LNCS 453, Springer, Berlin 1990, 246-264.

[Chau_92] David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

[CoBi_95] David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

[CTCPEC_92] Canadian System Security Centre; Communications Security Establishment; Government of Canada: The Canadian Trusted Computer Product Evaluation Criteria; April 1992, Version 3.0e.

[DoDS_83] Department of Defense Standard: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711.

[Fede_99] Hannes Federrath: Sicherheit mobiler Kommunikation; DuD-Fachbeiträge, Vieweg, Wiesbaden 1999.

[FeJP_96] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy; Information Hiding, 1st Workshop, Cambridge, UK, LNCS 1174, Springer, Heidelberg 1996, 121-135.

[GoRS_99] David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections; Communications of the ACM 42/2 (1999) 39-41.

[ITSEC_91] European Communities - Commission: ITSEC: Information Technology Security Evaluation Criteria; (Provisional Harmonised Criteria, Version 1.2, 28 June 1991) Office for Official Publications of the European Communities, Luxembourg 1991 (ISBN 92-826-3004-8).

[JMPP_98] Anja Jerichow, Jan Müller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol; IEEE Journal on Selected Areas in Communications 16/4 (May 1998) 495-509.

[KöPf_01] Marit Köhntopp, Andreas Pfitzmann: Informationelle Selbstbestimmung durch Identitätsmanagement; erscheint in: it+ti Informationstechnik und Technische Informatik, Themenheft "Sicherheit" 5/01; Oldenbourg Wissenschaftsverlag, München 2001.

[Pfit_90] Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Berlin 1990.

[Pfit_93] Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

[PfKö_01] Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; in: H. Federrath (Ed.): De-

signing Privacy Enhancing Technologies; Workshop on Design Issues in Anonymity and Unobservability, July 25-26, 2000, Intern. Computer Science Institute (ICSI), Berkeley, CA, LNCS 2009, Springer-Verlag, Heidelberg 2001, 1-9. aktuelle Version abrufbar unter http://www.koehntopp.de/marit/pub/anon/.

[PfWa_87] Andreas Pfitzmann, Michael Waidner: Networks without user observability; Computers & Security 6/2 (1987) 158-166.

[PPSW_99] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trustworthy User Devices; in: G. Müller, K. Rannenberg (Eds.): Multilateral Security in Communications, Addison-Wesley 1999, 137-156.

[PSWW_98] Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Guntram Wicke, Gritta Wolf, Jan Zöllner: A Java-based distributed platform for multilateral security; IFIP/GI Working Conference "Trends in Electronic Commerce", Hamburg, LNCS 1402, Springer, Heidelberg 1998, 52-64.

[PWP_90] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

[ReRu_99] Michael K. Reiter, Aviel D. Rubin: Anonymous Web Transactions with Crowds; Communications of the ACM 42/2 (1999) 32-38.

[ScPo_98] Michael Schneider, Ulrich Pordesch: Identitätsmanagement; Datenschutz und Datensicherheit DuD 22/11 (1998) 645-649.

[VoKe_83] Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM Computing Surveys 15/2 (1983) 135-171.

[WoPf_00] Gritta Wolf, Andreas Pfitzmann: Properties of protection goals and their integration into a user interface; Computer Networks 32 (2000) 685-699.

[WoPf_00d] Gritta Wolf, Andreas Pfitzmann: Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen; Informatik-Spektrum 23/3 (2000) 173-191.

3. Diskussionen im Begleitausschuss

Zur politischen und fachlichen Begleitung der zweiten Stufe der Novellierung des Datenschutzrechts wurde durch die Bundestagsabgeordneten Tauss (SPD) und Özdemir (Bündnis 90/Grüne) ein Begleitausschuss aus Mitgliedern des Deutschen Bundestages, Vertretern der Bundesregierung, Datenschützern des Bundes der Länder und von Unternehmen und Wissenschaftlern initiiert. Er traf sich im Januar 2001 zur Diskussion des Gutachtendesigns und im Juni 2001 zur Beratung eines Diskussionsentwurfs zum Gutachten. Die wichtigsten Anregungen und Bemerkungen aus der Begleitkommission sind im folgenden unkommentiert und ungewichtet als Thesen zusammengefasst:

3.1 Konstituierende Sitzung der Begleitkommission zum Gutachtendesign – Berlin 15.01.2001

Eine Regelung, die den Datenschutz vorrangig in einem zentralen Gesetz zusammenfassen und nur sehr begrenzt Ausnahmen in bereichsspezifischen Regelungen zulassen will, könnte mit dem Volkszählungsurteil und der Europäischen Datenschutzrichtlinie kollidieren, die eher sehr detaillierte Regelungen fordern.

Der Vorschlag eines expliziten Grundrechtsartikels zum informationellen Selbstbestimmungsrecht wird nach Prognose mehrerer Mitglieder der Begleitkommission – auch aufgrund einschlägiger Erfahrungen in der letzten Diskussion – an politischem Widerstand scheitern.

Ein künftiges Datenschutzrecht muss neben dem Schutz der Betroffenen auch den Schutz anderer Grundrechte (Meinungsfreiheit, Versammlungsfreiheit, Berufsfreiheit etc.) im Blick haben: Datenverarbeitung ist sozialadäquat und ebenfalls Ausübung von Grundrechten.

Informationsfreiheit muss gleichgewichtiges Schutzgut der Informationsverfassung neben der informationellen Selbstbestimmung sein. Sie bedarf daher eines „Ankers“ im Datenschutzrecht.

Die Definition der informationellen Selbstbestimmung muss klarstellen, dass es sich dabei nicht um eine Variante des Eigentumsrechts handelt, um der Kommerzialisierung personenbezogener Daten Einhalt zu gebieten.

Die Notwendigkeit einer Modernisierung des Datenschutzrechts ergibt sich neben dem daraus erwachsenden Wettbewerbs- und Standortvorteil vor allem aus dem Grundrechtsschutz und den Grundsätzen einer demokratischen Gesellschaft.

Eine „große Integrationslösung“ wäre wünschenswert, die auch die Telekommunikation in das neue BDSG integriert. Damit wären klarere Strukturen zu erreichen und die Durchsetzbarkeit würde erleichtert.

Die Trennung zwischen Datenverarbeitung und Telekommunikation macht keinen Sinn mehr, da der Großteil der Datenverarbeitung heute ohnehin unter Verwendung der Telekommunikation geschieht und dieser Trend weiter anhalten wird.

Alle bisherigen bereichsspezifischen Regelungen müssen bei der Entwicklung übergreifender Grundsätze berücksichtigt und einbezogen werden.

Die politische Intention, alle Datenverarbeitung in ein neues Datenschutzrecht einzubeziehen, wird momentan durch eigenständige Gesetzgebungsarbeiten z.B. im Bereich der genetischen Daten und im Telekommunikationsbereich konterkariert. Hier ist die Politik gefragt!

Das Verhältnis von Datenschutz zu anderen Rechtsgebieten (Urheberrecht, zivilrechtliche Geheimnisse etc.) muss geklärt werden.

Die Folgen der Aufgabe des Prinzips „Verbot mit Erlaubnisvorbehalt“ müssen klar dargestellt werden.

Das Verhältnis von Einwilligung und Erforderlichkeit muss ausgewogen sein.

Der hohe Wert der Zustimmung/Einwilligung ist angesichts der heutigen Technik zu hinterfragen.

Es ist daher notwendig, der Zustimmung klare Grenzen zu setzen! Die Zustimmung muss an Voraussetzungen geknüpft werden.

Die Gleichstellung von Zustimmung des Betroffenen und Erlaubnis/Anordnung durch ein Gesetz muss beendet werden.

Das künftige Datenschutzrecht muss die wachsende Abhängigkeit der Betroffenen von Datenverarbeitung berücksichtigen. Die Entscheidungsfreiheit bei der Zustimmung muss gewährleistet sein.

Datenschutzrecht sollte mehr auf Selbstbestimmung setzen. Dem Einzelnen muss überlassen werden, wieviel Datenschutz er will. Insoweit muss aber auch sichergestellt werden, dass der Einzelne von der Art der Datenverarbeitung und den verwendeten technischen Systemen Kenntnis hat.

Dabei muss allerdings berücksichtigt werden, dass das Verhalten des Nutzers von Sorglosigkeit und Übereilung geprägt ist. Das Idealbild des bewussten Nutzers entspricht nicht der Realität.

Der Wert der Zustimmung kann durch eine konsequente Zweckbindung erhöht werden.

Informierte Einwilligung setzt voraus, dass die Reichweite dieser Einwilligung erkannt wird.

Die Datenvermeidung muss „vor die Klammer gezogen“ werden. Damit wird auch der Umfang der Einwilligung begrenzt.

Pseudonyme sind der einzige Weg, um zu einer Minimierung des Personenbezugs zu gelangen. Wegen der Gefahr der Zusammenführung von Pseudonymen und der damit verbundenen Möglichkeit der Zuordnung zu Personen, müssen technische Regelungen zur Authentizität der Daten vorgesehen werden.

Die Unterscheidung zwischen gezielter und ungezielter Datenverarbeitung birgt die Gefahr einer schwer zu fassenden Klassifizierung konkreter Datenverarbeitung. (Ab) wann kommt es dem Datenverarbeiter auf den Personenbezug an?

Die Unterscheidung zwischen gezielter und ungezielter Datenverarbeitung ist sinnvoll, um das Datenschutzrecht im Bereich der Datenverarbeitung zu allein technischen Zwecken zu entlasten.

Die Unterscheidung zwischen zielgerichteter und nicht zielgerichteter Datenverarbeitung ist mit der Europäischen Richtlinie nicht vereinbar, da sie gegen die Zweckbestimmung verstößt. Ebenso verstößt diese Unterscheidung gegen das Grundrecht auf informationelle Selbstbestimmung, da sie den Bereich der nicht gezielten Datenverarbeitung dem Betroffenen unzugänglich macht (es fehlt dort selbst am Auskunftsrecht). Insbesondere Data-Mining darf nicht dem Einfluss des Betroffenen entzogen, d.h. auch nicht im Bereich der nicht gezielten Datenverarbeitung angesiedelt sein.

Den Bedenken gegen eine Unterscheidung von gezielter und ungezielter Datenverarbeitung könnte durch kurze Vorhaltungsfristen (Erforderlichkeit) im Bereich der ungezielten Datenverarbeitung entgegengetreten werden.

Die Einbeziehung juristischer Personen könnte im Bereich der technisch orientierten Verarbeitung sinnvoll sein.

Es ist fraglich, ob juristische Personen des gleichen Schutzes bedürfen wie natürliche, bei denen es um die Würde des Menschen und seine persönliche Entfaltung geht. Ein ver-

gleichbarer Eingriff durch die Datenverarbeitung ist bei juristischen Personen so nicht denkbar.

Die Einbeziehung juristischer Personen in den Schutzbereich wäre sinnvoll, wenn es sich um gemeinnützige juristische Personen handelt (Parteien, Vereine). Hier greife auch das Argument, dass damit kommerzielle Interessen geschützt werden, nicht.

Die „Sackgassenregelung" im Bereich der Zweckbindung sollte als Garantie der datenverarbeitenden Stelle vorgesehen werden.

Bei einer Ausweitung der Selbstregulierung muss klargestellt werden, dass es staatliche Aufgabe bleibt zu prüfen, ob diese Aktivitäten ausreichend sind.

Selbstregulierung sollte besser als „Co-Regulierung" (unter Einschluss bspw. der Verbraucher) gesehen werden. Bestimmte Leitentscheidungen für die Selbst (Co-) regulierung sollten im Gesetz vorgesehen werden. Die Finanzierung einer solchen Co-Regulierung muss sichergestellt werden.

In diesem Zusammenhang könnte an Allgemeinverbindlichkeitserklärungen gedacht werden.

Betriebliche und behördliche Datenschutzbeauftragte bedürfen einer besseren Qualifikation.

Für exekutive Befugnisse der Datenschutzbeauftragten bedarf es einer Grundgesetzänderung.

Anforderungen an Datenschutzkontrollen innerhalb der Unternehmen müssen erheblich verschärft werden.

Der Arbeitnehmerdatenschutz muss flankierend zum allgemeinen Datenschutzrecht modernisiert werden. Dies ist ein Appell an die Politik!

3.2 Statements von Mitgliedern der Begleitkommission zur Diskussionsfassung

Lösungsansätze zur Modernisierung des Datenschutzrechts

- Analyse und Überlegungen des Gutachtens finden volle Unterstützung, insbesondere die Stärkung der Einwilligung, des Selbstdatenschutzes und die zentrale Rolle, die das BDSG in Zukunft spielen soll.
- Gutachten orientiert sich noch zu sehr am alten Konzept der DV, das nur den Betroffenen auf der einen Seite und die verantwortliche Stelle auf der anderen kennt. Bereits heute gibt es im Rahmen der Auftrags-DV Funktionsübertragungen. Diese unterschiedlichen Funktionen einer intermediären DV müssen hinsichtlich der eigenen und fremden Inhalte der DV systematisiert werden.
- Es ist fraglich, ob die manuelle DV (insb. im nicht-öffentlichen Bereich) mit einbezogen werden sollte.
- Die Normierung der informationellen Selbstbestimmung als eigenständiges Grundrecht wird skeptisch gesehen, es besteht insoweit kein Handlungsbedarf, auch ist nicht klar, was ein solches konkret bewirken würde.
- Für eine Einschränkung der informationellen Selbstbestimmung in öffentlichem Interesse muss dieses auch überwiegen.
- Profilbildung darf für Detekteien nicht zu großzügig gehandhabt werden – entscheidender Unterschied zu bspw. BKA-Befugnissen.
- Die Datensammlung auf Vorrat sollte verboten werden.
- Marketing und Customizing bauen auf einem intensiven Personenbezug auf, dies muss berücksichtigt werden, Datenschutz kann die gesellschaftliche Produktionspraxis nicht ändern.

- Die Wirtschaft setzt auf die Personalisierung der Beziehung zwischen Unternehmen und Kunden. Es bedarf daher handhabbarer Einwilligungsprozeduren, "permission marketing".
- Eine zu hohe personelle und finanzielle Belastung der Wirtschaft durch Datenschutz-Audits könnte eine Gefahr für die Umsetzung sein.
- Vom Begriff des Datengeheimnisses sollte Abschied genommen werden, da dieser unerwünschte Assoziationen hervorruft (z.B. zu Geheimdiensten), es sollte simpel ausgedrückt werden, was es beinhaltet: der jeweilige Mitarbeiter darf nur die DV vornehmen, zu der er befugt ist.
- Sollten Datenschutz und Geheimnisschutz grundsätzlich getrennt werden, da es Auflösungserscheinungen hinsichtlich der Grenzen zwischen personenbezogenen Daten und Daten allgemein gibt? Insoweit könnte die Figur „DV ohne gezielten Personenbezug" ein Kompromiss sein (der allerdings dogmatische Probleme aufwirft).
- Zu den Aufgaben der Modernisierung des Datenschutzrechts (S. 13) sollte auch die Verlässlichkeit dessen, was in der DV geschieht, als Grundsatz der rechtmäßigen DV definiert werden (Datenverarbeiter muss für sichere und vertrauenswürdige DV sorgen).
- Auch für die Hersteller und Provider muss das Datenschutzrecht gelten, sie müssen "Angesprochene" sein.
- Die Sicherheit sollte integraler Bestandteil aller Technik sein.
- Datenschutz durch Technik sollte strafrechtlich flankiert werden.
- Es ist fraglich, ob Datenschutz die Technikentwicklung nachhaltig beeinflussen kann.
- Es ist eine strategische Frage, wie die Hersteller zur Entwicklung datenschutzgerechte Technik bewegt werden, eine hohe Sensibilität ist jedenfalls gegeben.
- Das Gutachten sollte sich nicht auf die TK-Richtlinie der EU beziehen, da diese noch in der Entwicklung ist und somit noch nicht präzise genug. Ähnliches gilt für P3P (S. 32), welches noch in der Entwicklung steht und einer materiellen Ausformung bedarf. Es sollte daher auch allenfalls modellhaft behandelt werden.
- Die Rolle der mehrseitige Sicherheit sollte noch mehr betont werden.
- Die Gleichstellung von juristischen mit natürlichen Personen wird begrüßt.
- Die Einbeziehung juristischer Personen ist ein fataler Fehler, da dadurch die Funktion des informationellen Selbstbestimmungsrechts als Partizipationsrecht und Grundlage der Demokratie in Frage gestellt wird. Wenn das TK-Recht in ein BDSG integriert werden soll, dann können Rechte juristischer Personen aus diesem Bereich auch auf diesen beschränkt werden. Im übrigen gibt es schon seit den fünfziger Jahren die Meinung von Zivilrechtlern, dass es sich bei der Rechtsfigur „juristische Person" um ein künstliches Gebilde handele.
- Es bestehen erhebliche Bedenken gegen die Einbeziehung juristischer Personen. Dafür fehlt aus Sicht der Wirtschaft der Bedarf. Darüber hinaus wäre dies mit einem großen Aufwand hinsichtlich der Auskunft und Benachrichtigung verbunden. Die gewollte Verschlankung und Vereinfachung würde ins Gegenteil verkehrt.
- Für die Einbeziehung juristische Personen besteht kein Handlungsbedarf. Insbesondere hat das BVerfG dies so auch nie festgestellt sondern vielmehr immer offen gelassen.
- Zuständigkeit der Kontrollstellen (Bund, Länder, EU) im nicht-öffentlichen Bereich sollte überdacht werden.
- Die Gesetzgebungskompetenz im Datenschutzrecht sollte künftig stärker beim Bund liegen. Dabei sollte auch auf machtpolitische Überlegungen eingegangen werden, wie z.B. der Datenschutz Vorrang gegenüber wirtschaftlichen Erwägungen (auch bezogen auf die Ressorts) erlangen kann.

- Der Zeitrahmen für die Umsetzung (Angleichung der bereichsspezifischen Gesetze) wird mit zwei Jahren zu gering bemessen sein.
- Formulierungsvorschläge von Gesetzestexten sollten im Gutachten enthalten sein.
- Gutachten sollte an einem konkreten Bereich, an konkreten Themenkomplexen die Entflechtung des Datenschutzrechts hin zu einem starken BDSG mit wenigen Ausnahmeregeln demonstrieren (Therapieart, bspw. für Zweckbindung, automatischer Abruf).
- Dem Gutachten fehlt teilweise Perspektive und Prognose: eine dritte Stufe der Modernisierung des Datenschutzrechts sollte angedacht werden, ebenso sollte die Entwicklung des EU-Rechts prognostiziert werden.
- Das Gutachten sollte noch innovativer sein, da die Vorschläge durch die praktische Politik ohnehin noch abgeschnitten werden.
- Datenschutz sollte auch in Zukunft ein föderativ gestaltetes Rechtsgebiet bleiben.
- Für den Erfolg des Gutachtens ist eine 8-10 seitige Fassung notwendig, die prägnant und konkret die entscheidenden Forderungen der Gutachter an die Politik benennt.

Anwendungsbereich des Gesetzes / Grundsätze der Datenverarbeitung

- Als Forschungsprivileg sollte auf das „erhebliche“ Überwiegen der Forschungsinteressen – im Hinblick auf die grundrechtlich garantierte Forschungsfreiheit – gegenüber dem Interesse des Betroffenen verzichtet werden. Die Verwendung des Datums führt nicht zu einer Intervention gegenüber dem Betroffenen, dieser ist vielmehr lediglich Merkmalsträger – von daher sind auch keine Nachteile zu erwarten. Besser wäre es, diese Daten durch ein weitergehendes Verwertungsverbot (Strafverfolgung, Beschlagnahmeverbot) zu schützen.
- Für die DV im Rahmen der Forschung auch ein „erhebliches Überwiegen“ des Forschungsinteresses gegenüber dem des Betroffenen vorzusehen, entspricht den sonstigen Abwägungsregeln und sollte deshalb beibehalten werden, zumal es zu Schwierigkeiten in der Nachprüfbarkeit kommen wird, da der Forscher seinen Forschungsgegenstand immer selbst bestimmt. Insoweit ist diese Hürde ein Ausgleich dafür, dass die Forschung an sich nicht nachprüfbar ist.
- Auf S. 57 sollte klargestellt werden, dass eine Übermittlung nicht nur bei einem Anspruch sondern bereits bei einer Befugniss der übermittelnden Stellen zulässig ist.
- Im öffentlichen Bereich muss genau unterschieden werden zwischen der Befugnis und den Aufgaben der Stelle die die DV legitimieren sollen. Stellt man nur auf die Aufgaben ab, so öffnet sich eine gefährliche Flanke, da diese in bestimmten Bereichen nahezu jegliche DV legitimieren würden. Die Erforderlichkeit der DV muss eng mit dem Zweck verknüpft werden.
- Die Löschungspflichten sollten präzisiert (3 Jahre), Verstöße als Amtspflichtverletzung geregelt werden.
- Die DV ohne gezielten Personenbezug ist ein gravierender und wichtiger Ansatz. Probleme wird es bei der Abgrenzung zwischen den beiden Kategorien geben. Für die Ahndung von Missbrauch sind Bußgeldvorschriften nicht ausreichend.
- Nach wie vor ist die Kategorie „DV ohne gezielten Personenbezug“ nicht überzeugend. Nur wenn ganz klar ist, dass auf diese Daten nicht anderweitig zurückgegriffen werden kann (z.B. durch Staatsanwaltschaft, Polizei), könnte man sie u.U. akzeptieren.
- Das Gutachten statuiert zwar die Aufgabe des Verbots mit Erlaubnisvorbehalt, der Vorschlag, statt dessen Grundsätze als Voraussetzung einer rechtmäßigen DV zu normieren, läuft aber faktisch auf dasselbe hinaus.
- Wenn auch das Ergebnis ein ähnliches ist, so entspricht dieser Ansatz der Informationsgesellschaft und ist richtig.

- Für die Zulässigkeit der DV im nicht-öffentlichen Bereich grundsätzlich die opt-in-Lösung vorzusehen führt zu Problemen bei der globalen DV im Internet. Die Anforderungen in Deutschland können nicht in allen Ländern erfüllt werden. Sie entsprechen auch nicht den bisherigen Beratungen im Global Business Dialog. Daher sollten für Marketingzwecke Differenzierungen erfolgen (bspw. Adressen für einfache Werbung privilegieren). Dies würde auch zu einer höheren Akzeptanz in der Wirtschaft führen.
- Die Aufwertung der Einwilligung als Legitimationsgrundsatz der DV sollte nicht zu weit gehen, insbesondere im öffentlichen Bereich.
- Die vorgesehenen Ausnahmen für eine Einwilligung als Voraussetzung der DV sind zu eng gefasst: „berechtigtes Interesse“ ist häufig ausreichend, listenmäßig zusammen gefasste Daten sollten auch ausgenommen werden – ansonsten sind Widerstände u.U. nicht zu überwinden.
- Es verbleiben Anwendungsbereiche, in denen ein „opt out“ ausreichend ist.
- Die Einwilligung sollte generell zeitlich begrenzt sein, nach Ablauf eine erneute Einwilligung eingeholt werden müssen. Nur so kann der Betroffene wissen, wozu er seine Einwilligung gegeben hat.
- Für die Form der Einwilligung sind §§ 126, 126a BGB ausreichende Grundlage.
- Die Altersregel für die Einwilligung im Internet (16 Jahre, S. 43) sollte an andere Altersbegrenzungen (GR-Mündigkeit 14 Jahre) angeglichen werden, da sonst eine neue Altersgrenze eingeführt wird, die einer besonderen Begründung bedürfte.
- Der Begriff „personenbezogene Daten“ muss im Zusammenhang mit pseudonymen Daten genauer definiert werden.
- Die Differenzierung, dass pseudonyme Daten nicht personenbezogene Daten (S. 48) sind, wirft Bedenken auf, da auch pseudonyme Daten mit dem erforderlichen Zusatzwissen zumindest personenbeziehbar sein können.
- Bei Teil 3, 3.4.3 (S. 48) fehlt die weiter hinten im Diskussionsentwurf erfolgte Abstufung der Pflichten zur anonymen, pseudonymen etc. DV. Dies ist aber wichtig, da die Verkettbarkeit pseudonymer Daten zu Aufdeckungsmöglichkeiten führt.
- Die Datenschutzerklärung muss Transparenzaspekte in den Vordergrund stellen. Verstöße dagegen sollten als Ordnungswidrigkeit sanktioniert werden. Für Mindestanforderungen an die Datenschutzerklärung können Vorgaben des Europarats für Online-Datenschutzerklärungen dienen, ebenso entsprechende Regelungen der OECD.
- Solche Anforderungen an Privacystatements entsprechen nicht der Praxis, da diese Statements nicht verbindlich sind, sondern nur eine Unternehmenspolicy wiedergeben.
- Die Unterscheidung zwischen elektronischer und manueller (auf Papier) DV ist nicht mehr möglich. Durch Scanner ist potenziell alles elektronisch.

<u>Datenschutzmanagement</u>

- Das Datenschutz-Audit-Gesetz sollte jetzt (unabhängig vom BDSG) umgesetzt werden.
- Die Überlegungen zum Outsourcing (S. 58 f) sind nicht überzeugend. Die Regelungen für die Auftragsdatenverarbeitung sind in der Praxis ausreichend und besser, als eine neue Kategorie einzuführen.
- Datenschutzkonzepte (S. 63, 64) sollten nicht nur für ganze Unternehmen sondern auch für einzelne Teilbereiche möglich sein.
- Das Grundschutzhandbuch des BSI ist sehr öffentlich-lastig und als Grundlage für den nicht-öffentlichen Bereich nicht geeignet.
- Die Begrifflichkeit zu Datenschutzmanagementsystem, DS-Konzept und DS-Organisationsplan ist unklar.

- Es bedarf eines Konfliktlösungs-Mechanismus‘ bei Unstimmigkeiten zwischen betrieblichen Datenschutzbeauftragten und Datenschutz-Auditoren.

Selbstregulierung

- Der Selbstregulierungsgrundsatz wird begrüßt, allerdings sind die Anreize für die Wirtschaft, davon Gebrauch zu machen, noch nicht richtig ersichtlich, wenn die Regelungen Grundlage von Kontrollen und Schadensersatzforderungen sein könnten. Auch die Frage der Durchsetzung von Schadensersatzansprüchen ist noch nicht ausreichend geklärt.
- Die Durchsetzung von Verhaltensregeln (6.5.3) sollte nicht abschreckend wirken, wenn nämlich diejenigen, die mehr tun, höher bestraft werden können. Es muss hinsichtlich der Sanktionen eine klare Schnittstelle zwischen Gesetz und Selbstregulierung geben.
- Im Gutachten fehlt bei der Situationsanalyse, dass Datenschutz ein Wettbewerbsvorteil sei, eine Auseinandersetzung mit der (falschen) Auffassung, Datenschutz sei ein Wettbewerbsnachteil (u.a. wegen finanzieller Belastungen).
- Für die Selbstregulierung muss mehr Verbindlichkeit geschaffen werden.
- Eine Allgemeinverbindlichkeitserklärung ist angesichts des „ausgehandelten“ Gesetzgebungsprozesses im Atomaustiegsvertrag auch für den Bereich des Datenschutzes möglich.
- Das Wettbewerbsrecht für Zwecke des Datenschutzes zu nutzen, ist eine gute Idee.
- Als Adressaten der Selbstregulierung (S. 70) sollten auch Unternehmen aufgenommen werden.
- Die Veröffentlichung von Regelungen der Selbstregulierung im Amtsblatt geht zu weit. Sie sollte vielmehr unternehmensbezogen erfolgen.

Betroffenenrechte

- Die Privilegierung nicht-öffentlicher Stellen im Haftungsrecht muss aufgegeben werden.
- Die Beweislastumkehr und der Ersatz immaterieller Schäden wird kritisch betrachtet.
- Die Gleichstellung von Übermittlung und Veröffentlichung ist angesichts von Interneteinstellungen von Registern etc. problematisch.
- Das Auskunftsrecht (S. 79 / 80) darf nicht zu einer Preisgabe von Betriebsgeheimnissen führen, auch im Hinblick auf die Struktur der DV. Es besteht die Gefahr der Ausforschung durch Konkurrenten.
- Die Gefährdungshaftung wird abgelehnt. Deckungsvorsorge würde zu erheblichen Kosten (Versicherungsprämien) führen. Wenn überhaupt, müssen Serienschadensklauseln und Höchstgrenzen vorgesehen werden.
- Hinsichtlich der Gefährdungshaftung bedarf es einer Differenzierung. Ein Handwerksbetrieb wäre u.U. in seiner Existenz bedroht.

Technik und Organisation

- Bzgl. Pseudonymität sind mindestens zwei Ebenen zu unterscheiden:

  - Anwenderebene: Hier kann Pseudonymität manchmal gewünscht sein, hin und wieder aber auch gar nicht, z.B. Personalisierung im customer relationship management

  - Netzebene: Hier ist Pseudonymität immer gewünscht.
- Pseudonymisierung ist nicht die Lösung für alles, vielmehr sollte die Datensparsamkeit (Vermeidung von Datenspuren) immer im Vordergrund stehen.
- Die rückwirkende Personalisierung muss ausreichend geklärt sein, da Daten so zu personenbeziehbaren werden können.
- Die technische Unterstützung der Zweckbindung wird sich schwierig gestalten, da der Zweck von der Technik nicht erfasst wird.

Datenschutzkontrolle

- Die Institution eines Konzerndatenschutzbeauftragten sollte eingeführt werden. Dies führt zu einer besseren Ausstattung und zu höherer Kompetenz des jeweiligen Amtsinhabers.
- Der Vorschlag, die Kontrollstellen für den öffentlichen und nicht-öffentlichen Bereich zusammenzuführen, wird begrüßt. Das führt zu Synergieeffekten.
- Die Argumente des Gutachtens zur Zusammenlegung der Kontrollstellen sind nur bedingt überzeugend. Sie könnten gegen jegliche differenzierte Behördenordnung sprechen. Funktionelle Differenzierung ist aber sinnvoll.
- Zwangsbefugnisse im öffentlichen Bereich sind problematisch. Das Gutachten sollte zumindest auf die Bedenken dagegen eingehen.
- Für eine verwaltungsrechtliche Konkurrentenklage könnte das Umweltrecht als Vorbild dienen.
- Die Rechtsqualität der Kontrollstelle, wie sie das Gutachten vorsieht, legt eine Stellung als Verfassungsorgan nahe, was problematisch ist. Im Vergleich mit anderen Beauftragten wird dies deutlich. Weniger kann manchmal mehr sein. Das Geheimnis des Erfolgs der Datenschutzbeauftragten ist deren Überzeugungskraft.
- Es wäre verfassungswidrig, wenn Datenschutzbeauftragte anderen Behörden Anweisungen geben könnten.
- Das Selbstverständnis und die Unabhängigkeit des Datenschutzbeauftragten wäre mit einer Erweiterung von Befugnissen nicht mehr gegeben.
- Eine Aufhebungsmöglichkeit von Entscheidungen des Datenschutzbeauftragten durch das Gericht würde die Unabhängigkeit schwächen. Ausreichend und wirksam ist vielmehr der enge Kontakt zum Parlament.
- Im nicht-öffentlichen Bereich würde die Beratungsfunktion durch gerichtliche Auseinandersetzungen verdrängt.

---

4. Workshops zum Gutachten

Begleitend zur Erstellung des Gutachtens fanden mehrere fachspezifische Konferenzen und Workshops mit Interessen- und Fachverbänden und verschiedenen Datenschutzinstitutionen statt, um so früh wie möglich Anregungen und Wünsche einer breiten Fachwelt und Öffentlichkeit in die Gestaltung des künftigen Datenschutzrechts einfließen zu lassen.

Am 23. Februar 2001 trafen sich die Gutachter mit den Mitgliedern des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik. Ein Workshop am 5. März 2001 in Berlin widmete sich den Interessen und Anliegen der Wirtschaft. Daran teil nahmen Mitglieder des Arbeitskreises Datenschutz der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. und der Gesellschaft für Datenschutz und Datensicherung e.V. Im Mittelpunkt des Workshops am 14. März 2001 in Bonn standen die Interessen von Verbraucher-, Berufs- und Datenschutzverbänden und Informatikvereinen sowie Fragen des Arbeitnehmerdatenschutzes. Am 2. April 2001 besuchten die Gutachter das Bundesamt für Sicherheit in der Informationstechnik in Bonn, um mit Experten verschiedener Bereiche des Amtes technische Fragen des Datenschutzes zu diskutieren. Die Lösungsvorschläge des Gutachtens wurden schließlich am 3. und 4. April 2001 in Düsseldorf von den Datenschutzbeauftragten der Länder und des Bundes beraten.

Die wichtigsten Anregungen und Bemerkungen der Workshops sind im folgenden unkommentiert und ungewichtet als Thesen zusammengefasst.

4.1 Workshop mit dem Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik am 23. Februar 2001

- Es gibt kein allgemeingültiges Modell der Datenverarbeitung, also auch kein allgemeingültiges Modell des Datenschutzes mehr.
- Die Intelligenzentwicklung in der Technik (z.B. intelligente Agenten) stellt den Datenschutz vor neue, auch unvorhergesehene Probleme. Dies muss im Gutachten benannt werden.
- Durch die fortschreitende Vernetzung und Geschwindigkeit in der Datenverarbeitung wird die Zweckbindung in den nächsten 10 Jahren immer mehr gefährdet sein.
- Gesetz muss daher robust gegenüber unvorhergesehenen technischen Entwicklungen sein. Die datenschutzrechtliche, abstrakte Zielsetzung muss im Mittelpunkt stehen. Die jeweils verwendete Technik muss sich darauf im konkreten Fall einstellen. Konkrete technische Maßnahmen sind nur dort im Gesetz festzuhalten, wo es unvermeidbar ist.
- Falls technische Maßnahmen im Gesetz benannt werden, dann muss auch klargestellt sein, dass im Zuge der Weiterentwicklung des Standes der Wissenschaft und Technik der Ersatz der vorgeschriebenen Maßnahmen durch wirkungsvollere erlaubt – ggf. gefordert – ist.
- Die Aufgabe der Informationstechnik darf nicht auf die Datensicherheit beschränkt werden, sondern muss auch die Gestaltung der Datenverarbeitung selbst umfassen.
- Zu klären ist die Verantwortlichkeit / Zurechenbarkeit bei der Datenverarbeitung: Hier gibt es verschiedene Ebenen: Provider, Nutzer, Generator der Daten, Dienste, Softwarehersteller etc. Wie könnte ein System informationeller Garantien zu gestalten sein? (Gibt es eine Rechtspersönlichkeit von Maschinen?) Möglicherweise ist auch der Begriff „verantwortliche Stelle“ nicht mehr scharf genug.
- Dabei ist zu berücksichtigen, dass das Datenschutzrecht kein allgemeines Informationsverarbeitungsgesetz sein kann.
- Verantwortlichkeit muss *an Personen* angeknüpft werden.
- Welche Instanz kann die Kontrolle ohne Eigennutz gewährleisten?
- Sollte weiterhin zwischen personenbezogenen und personenbeziehbaren Daten unterschieden werden oder nicht?
- Die Information des Betroffenen über die Verarbeitung seiner Daten muss verstärkt werden.
- Die Verarbeitungsweise personenbezogener Daten kann auch Verhandlungssache sein. Dann aber müssen die Beteiligten über die Konsequenzen informiert sein. Hierzu bedarf es auch einer anfänglichen, geschützten Experimentierphase.
- Welche Grenzen (Tabuzonen) gibt es in der Verhandlungsmasse und wer verhandelt: der Mensch oder die Maschine? Wie wirkt es sich aus, dass das informationelle Selbstbestimmungsrecht ein Grundrecht ist?
- Die Durchsetzung des Datenschutzes kann durch eine Überwachung von unabhängigen Stellen oder durch die Betroffenen selbst erfolgen. Dort wo die Beteiligten selbst handeln können, sollte die Überwachung (als ultima ratio) zurücktreten.
- Der Begriff „open source“ definiert die Zielstellung ungenau, er ist nicht deckungsgleich mit Transparenz: Die Offenlegung der Quellen (preferred representation) und Generatoren, sollte daher nach dem NRW-Modell als „Nachvollziehbarkeit mit angemessenem Aufwand“ bezeichnet werden.

- Die Aufgabe des Prinzips „Verbot mit Erlaubnisvorbehalt“ und dessen Ersetzung durch einzuhaltenden Grundsätzen der Verarbeitung personenbezogener Daten ist konsequent, da dieses in der heutigen Datenverarbeitung ohnehin nicht mehr zum tragen kommt (kommen kann).
- Die Unterscheidung zwischen gezielter und ungezielter Verarbeitung personenbezogener Daten ist problematisch und ggf. konkreter zu definieren. Auch bei Data-Mining wissen die Anwender bereits, wofür sie bestimmte Daten sammeln.
- Explizite Aussagen zu den Grenzen der Videoüberwachung sollten im Gutachten enthalten sein.
- Die Zugriffsmöglichkeiten des Betroffenen auf seine Daten müssen gestärkt werden.

4.2 Workshop mit Vertretern der Wirtschaft am 5.3.2001 Berlin

Im Mittelpunkt standen insbesondere die folgenden acht Themenkreise:

1. Stärkung der Zustimmung setzt **Stärkung ihrer Freiwilligkeit** voraus,
2. **Grundmodelle der Selbstregulierung**,
3. Erhöhung der **Transparenz** der Datenverarbeitung,
4. Verfahren bei **Zweckänderungen** (Übermittlung),
5. Gesonderte Kategorie: **ungezielte Datenverarbeitung** (z.B. Kommunikation zwischen Maschinen, Datenanfall nur für technische Prozesse),
6. Einbeziehung **juristischer Personen** in das Datenschutzrecht,
7. Künftige Rolle des **betrieblichen Datenschutzbeauftragten**,
8. **Technische oder organisatorische Maßnahmen** zur Umsetzung der strikten Zweckbindung.

1. Freiwilligkeit der Zustimmung

- Wie wird Freiwilligkeit definiert? Ist die Zustimmung noch freiwillig, wenn eine Ablehnung zu einer komplizierteren/individuellen Datenverarbeitung führt, die mehr Kosten – auch für den Betroffenen – verursacht?
- Modellklauseln sind eine Frage der Machbarkeit, eine individuelle Aushandlung von Datenschutzklauseln ist vor allem im Massengeschäft nicht praktikabel.
- Voraussetzung einer Stärkung der Freiwilligkeit der Zustimmung ist die Aufgabe des Prinzips „Verbot mit Erlaubnisvorbehalt“. Dahingehende Vorschläge werden begrüßt.
- Die Einwilligung sollte im Gesetz als Grundsatz benannt, die detaillierte Ausformung aber der Selbstregulierung überlassen sein.
- Die konkrete Form der Datenverarbeitung und -übermittlung (Post oder elektronische Übermittlung) sollte vom Verarbeiter selbst gewählt werden dürfen, ohne dass dies einer erneuten Einwilligung bedarf (z.B. im Bereich der Personaldatenverarbeitung). Voraussetzung ist eine ausreichende technische Absicherung.
- Freiwilligkeit der Zustimmung im Geschäftsverkehr ist eigentlich kein Problem, da Privatautonomie beiderseitige Freiwilligkeit ohnehin voraussetzt.
- Gesetzliche Regelungen und internationale Abkommen verlangen von Banken die Sammlung weitergehender Daten, z.B. für verpflichtende ratings. Bedarf es hierzu einer gesonderten Einwilligung?
- Datenschutzrecht dient der Absicherung des Schwächeren. Daher muss die Freiwilligkeit auch materiell gegeben sein.

- Grundbestand an notwendigen Daten für die Vertragserfüllung könnten per Selbstregulierung (branchenspezifisch) festgeschrieben werden.
- In der Grundversorgung darf es zu keinen zusätzlichen Kosten kommen, wenn einer weitergehender Datenverarbeitung (über den Vertragszweck hinaus) nicht zugestimmt wird: Beispiel schufaloses Girokonto.

2. Selbstregulierung und deren Verbindlichkeit

- Beispiele für Selbstregulierung:
  · Konkretisierung rechtlich anerkannter Interessen;
  · Konkretisierung der Erforderlichkeit;
  · Konkretisierung von Zweckbestimmungen;
  · Grundsätze für branchenspezifische Unterrichtung von Betroffenen;
  · Konkretisierung für Ausnahmen von der Unterrichtung;
  · branchenspezifische Datenschutzerklärungen;
- Selbstregulierung ist der attraktivste Vorschlag des Designs.
- Für Gesetzgeber könnte eine gut funktionierende Selbstregulierung ein Anreiz sein, auf detaillierte Regelungen zu verzichten.
- Zielvorgaben für die Selbstregulierung sollten im Gesetz festgehalten, die Umsetzung den Interessenten branchenspezifisch überlassen werden. Dies vermindert Formalismen.
- Es muss geklärt werden, ob Maßnahmen im Rahmen der Selbstregulierung sowohl durch einzelne Unternehmen als auch durch ganze Branchen erfolgen können.
- Angesichts des Aufwands der Selbstregulierung (Kosten-Nutzen-Rechnung) ist es zweifelhaft, dass kleine und mittlere Unternehmen an eigenständiger Selbstregulierung interessiert sind. Hier sind die Verbände gefragt.
- Den Datenschutz weitgehend der Selbstregulierung zu überlassen, kann auch die Gefahr bergen, dass er nicht ernst genommen wird (These: Selbstregulierung bedeutet Nichtregulierung). Die Industrie wird bei Selbstregulierung versagen.
- Sollte Selbstregulierung gesetzesausfüllend oder gesetzesersetzend sein?
- Ein Gesetz muss der Selbstregulierung genügend Spielraum lassen.
- Es muss dafür gesorgt werden, dass Genehmigungen von Vorgaben der Selbstregulierung durch Kontrollstellen weitestgehende Gültigkeit haben (Länder, Bund, Europa). Eine neue Bürokratisierung ist zu vermeiden.
- Mit wem ist ein *code of conduct* abzustimmen? *Ein* Ansprechpartner für europaweite Geltung.
- Wenn Regelungen der Selbstregulierung von Unternehmen nicht für verbindlich erklärt werden, treten an deren Stelle die gesetzlichen Bestimmungen. Es ist dann Sache der Kontrollstellen, diese im Einzelfall auszulegen.
- Für die Durchsetzung verbindlicher Regeln bieten sich Bestimmungen des unlauteren Wettbewerbs an. Ansonsten ist auf Straf- und Ordnungswidrigkeitsbestimmungen im BDSG (z.Zt. § 43) zurückzugreifen.
- Der Forderung*, Codes of conduct* müssen maschineninterpretierbar sein, wurde entgegengehalten, dass die technische Umsetzung nicht zu hohe Kosten verursachen dürfe.
- Für die Industrie ist Datenschutz kein Wettbewerbsfaktor.

3. Transparenz

- Eine Transparenz der Datenverarbeitung ist grundsätzlich notwendig, darf aber unternehmerische Interessen nicht verletzen und auch nicht in Interna der betrieblichen Prozesse

eingreifen. Bei einer Offenlegung des Quellcodes besteht aber für manche Programme diese Gefahr.

- Die Offenlegung der Quellcodes gegenüber vertrauenswürdigen Dritten (öffentliche/private Kontrollstellen), die die Struktur der DV beurteilen können, könnte die generelle Offenlegung ersetzen. (Ombudsmannfunktion)
- *Einwand:* Junge Generation will sich selbst direkt informieren und dies nicht Dritten überlassen.
- Gütesiegel von vertrauenerweckenden Institutionen können weiterhelfen, dabei aber auf wenige beschränken.
- Die Offenlegung des Quellcodes ist national wegen des globalen Wettbewerbs nicht durchsetzbar.
- Adressat der Transparenz ist der durchschnittliche Nutzer, d.h. der Nichtinformatiker (vgl. Art. 12 DSRiLi).
- Transparenz ist Vertrauensfaktor. Die Nichtbeachtung der Transparenz könnte sanktioniert werden.

4. Zweckänderung

- Die Einholung einer nachträglichen, weitergehenden Einwilligung aufgrund sich ändernder Techniken und Rahmenbedingungen eines Vertrages (Bsp. Schufa) ist praktisch unmöglich.
- Könnte in diesem Fall Schweigen als Zustimmung normiert sein (Widerspruchslösung)?
- In diesen Fällen könnte eine Abstimmung mit Aufsichtsbehörden ein gangbarer Weg sein.
- Wirtschaft ist für „Sackgassenregelungen". Sie hat an unbeschränkter Weitergabe gar kein Interesse, denn irgendwann sind die Daten bei der Konkurrenz.
- Die Kontrollstellen könnten auch in diesem Bereich als „Ombudsmänner" fungieren.

5. Ungezielte Datenverarbeitung

- Zur „ungezielten" Datenverarbeitung könnten zählen:
  · Daten die ausschließlich der technischen Dienstleistung dienen (Verbindungsdaten),
  · Maschinen kommunizieren mit Maschinen,
  · Suchfunktionen im web.
- In diesen Fällen könnte die Unterrichtung, Auskunft, Zustimmung etc. entfallen. Voraussetzung dafür sind aber Datensparsamkeit, strikte Zweckbindung und die zügige Löschung sowie die Sicherstellung, dass es sich tatsächlich um ungezielte Datenverarbeitung im obigen Sinne handelt.
- Unterscheidung zwischen gezielter und ungezielter Datenverarbeitung wird von Wirtschaft grundsätzlich begrüßt.
- Wie verläuft die Abgrenzung? Bsp.: log files werden nur angelegt, weil dies gesetzlich gefordert ist. Handelt es sich dabei um eine zielgerichtete Verarbeitung personenbezogener Daten im Sinne des Vorschlags?

6. Juristische Personen

- Überlegungen zur Einbindung juristischer Personen in den Schutzbereich des BDSG sind aus einer Vereinheitlichung mit dem Telekommunikationsrecht entstanden.
- Aus Sicht der Wirtschaft ist dies nicht notwendig. Dort wo erforderlich besteht eine Einbeziehung bereits heute.
- Es besteht ein materieller Unterschied zwischen juristischen und natürlichen Personen. Juristische Personen bedürfen nicht des gleichen Schutzes wie natürliche. Hier reicht der Schutz von Geschäftsgeheimnissen.

- Abgrenzung ist aber häufig schwierig. In der Praxis enthalten Dateien über juristische Personen in der Regel auch Daten zu natürlichen Personen. Einbeziehung wäre die ehrliche Lösung.
- Ethisch-philosophischer Ausgangspunkt des Datenschutzrechts, der sich an den Persönlichkeitsrechten ausrichtet, passt nicht auf juristische Personen.
- *Replik*: Das Datenschutzrecht hat sich zu einem Verkehrsrecht des Informationszeitalters entwickelt.
- Die Einbeziehung juristischer Personen könnte zu einer Unzulässigkeit von Wirtschaftsauskunftsdateien, Informationsbroschüren etc. über juristische Personen führen.
- Es entsteht ein wesentlich umfangreicherer Aufwand im Bezug auf die Unterrichtung.

7. Betriebliche Datenschutzbeauftragte

- Die Position, Bedeutung und Unabhängigkeit des bDSB muss klarer definiert werden. Er muss auch Beschwerdeinstanz werden.
- Im Rahmen einer Stärkung der Selbstregulierung kommen auf den betrieblichen Datenschutzbeauftragten (bDSB) neue Aufgaben zu.
- Das Qualifikationsniveau muss angehoben, die Fachkunde muss verbessert werden. Hierzu bedarf es der Definition inhaltlicher Anforderungen an die Qualifikation.
- Die Fähigkeiten müssen unternehmensbezogen ausgestaltet sein.
- Eine Zertifizierung der Fachkunde ist nicht notwendig, statt dessen sollte das Datenschutzniveau in einem Unternehmen durch die Aufsichtsbehörde geprüft werden. Daraus lassen sich Schlüsse auf die Fachkunde des bDSB ziehen.
- Die Aufsichtsbehörden sollten dann das Recht haben, konkrete Anforderungen (auch an den Zeitaufwand für die Tätigkeit) zu stellen.
- Bei Anforderungen an die Fachkunde muss die Verhältnismäßigkeit im Auge behalten werden (Mittel-Zweck Relation, Betriebsgröße).
- Die Schwelle für bDSB (Mitarbeiteranzahl) könnte angehoben werden. Damit einhergehen könnten dann aber höhere Anforderungen, die klar zu definieren sind.
- Ein Anheben der Schwellenzahl kann zu outsourcing führen.
- Eine Obergrenze bei der Mitarbeiterzahl, ab welcher hauptamtliche bDSB zu bestellen sind, sollte nicht festgelegt werden.
- Der arbeitsrechtliche Kündigungsschutz für bDSB muss verbessert werden.
- Das Verhältnis zum Betriebsrat muss i.S.d. BAG geklärt werden.
- Unter Umständen wäre eine Gremiumslösung statt dem Ombudsmann-Modell vorteilhaft.
- Die Einführung eines „Konzerndatenschutzbeauftragten“ könnte zur besseren Durchsetzung konzernweiter Regelungen führen, wäre wirtschaftlich effektiver und wirtschaftsfreundlich, nicht zuletzt im Hinblick auf Marketingzwecke.

4.3 Workshop mit Vertretern von Verbraucher-, Berufs- und Datenschutzverbänden, Informatikvereinen und Experten im Arbeitnehmerdatenschutz am 14. März 2001

Selbstdatenschutz

- Derzeit wird gern vom Leitbild des informierten Verbrauchers ausgegangen (Wettbewerbsrecht, Rechtsetzung, EuGH, BGH, sonst. Rechtsprechung). Dies berücksichtigt nicht die unterschiedlichen Fähigkeiten der Verbraucher, das untere Drittel der Bildungspyramide wird ausgeblendet.

- Der durchschnittliche Verbraucher möchte sich nicht ständig um alle Informationen bemühen. Es muss ein Recht zur Flüchtigkeit geben. Auch der BGH spricht vom „flüchtig aufmerksamen Verbraucher". Hierauf muss das Datenschutzrecht eingehen. Insoweit Konflikt mit vorgesehener Stärkung der Zustimmung und Selbstschutz?
- Menschen reagieren nur auf wahrnehmbare Gefahren. Kaum jemand nutzt die Möglichkeiten des Selbstdatenschutzes, selbst wenn die Gefahren bekannt sind. Die persönlich Einstellung zum Datenschutz ist sehr flexibel, das tatsächliche Verhalten wiederum sehr inflexibel.
- Es bedarf einer eigenen Didaktik für den Umgang mit virtuellen Gefahren.
- Ein Schulfach zum Datenschutz in der Technik ist kontraproduktiv: Richtiger Umgang sollte spielerisch erlernt werden.
- Selbstdatenschutz betrifft die allgemeine Frage nach der Fürsorgepflicht des Staates: Diese ist beschränkt und muss auch beschränkt bleiben. Menschen müssen auch selbstverantwortlich, bewusst handeln (Bsp.: die „richtige Versicherung").
- Dies setzt Qualifizierung voraus, z.B. mehr Kapazitäten bei den LfD. Dabei müssen diejenigen, die den Qualifizierungsbedarf verursachen, diesen auch finanziell tragen. Dies muss gesetzlich geregelt werden, da wirtschaftlich daran kein Interesse bestehen wird.
- Dies würde eine „Bit-Steuer" oder eine Geräteabgabe bedeuten. (Gutscheine für Beratung beim Erwerb von Hard- und/oder Software).
- Qualifizierung zum effektiven Datenschutz sollte nicht staatlich unterstützt werden, auch nicht durch Bit-Steuer, sondern Haftungs- und Schadensersatzregelungen sollten dazu zwingen (vgl. Straßenverkehrserziehung).
- Mechanismen, die die menschliche Natur beim Selbstdatenschutz berücksichtigen, könnten sein:
  · verpflichtender Basisschutz für Datenverarbeiter,
  · Vereinfachung der Nutzung von Technik im Rahmen des Selbstdatenschutzes (unkomplizierte Installierung),
  · Standardlösungen rechtlich vorgeben oder den Rahmen dafür schaffen,
  · kollektive Interessen berücksichtigen und kollektive Rechtsdurchsetzung, die auch für die private
  Rechtsdurchsetzung notwendig ist, zulassen (Verbandsklage, vgl. § 22 AGBG),
  · kollektives Haftungsrecht, wenn Einzelschädiger nicht feststellbar.
- Probleme des Haftungsrechts sind aber folgende:
  Betroffener bemerkt den Schaden / Eingriff häufig gar nicht,
  Datenverarbeitung geschieht weltweit, insoweit führen einzelstaatliche Regelungen nur sehr begrenzt zum Ziel,
  Schadensersatz kann den angerichteten Schaden oft nicht mehr ausgleichen,
  es ist oft unklar, was eigentlich ein Verstoß ist, da das jeweilige System noch gar nicht verstanden wird.
- Weitere Instrumentarium wären die Anerkennung immaterieller Schäden bei Verletzung von Datenschutzregelungen, Mechanismen des UWG und Formulareinwilligungen, die mit Verbraucherverbänden und Kontrollstellen abgestimmt sind.

Verfassungsrang des Datenschutzes

- Für eine explizite Aufnahme des Datenschutzes in das GG sprechen dessen Verankerung in zehn Landesverfassungen und in der europäischen Grundrechtscharta.

- Die Zeit ist (nach verschiedenen erfolglosen Versuchen) reif. Mittlerweile ist allen klar, dass wir in einer Informationsgesellschaft leben. Die Geschichte des Staatsziels „Umweltschutz“ zeigt, dass es mehrerer Anläufe bedarf.
- Ein Datenschutzgrundrecht ist Gestaltungselement der Informationsgesellschaft.
- CDU muss eigentlich dafür sein, angesichts der Rolle Roman Herzogs im Entstehungsprozess der Grundrechtscharta der EU.
- Ein entsprechender Artikel darf nicht hinter die Aussagen des BVerfG im Volkszählungsurteil zurückfallen.
- Eine unmittelbare Drittwirkung sollte nicht explizit verankert sein. Es ist ausreichend, wenn die objektiven Werte herauskristallisiert werden – passfähig zum BVerfG – mit einem Schutzauftrag an den Staat. Ansonsten setzt man sich unnötigerweise der Kritik und dem Widerstand der konservativen Staatsrechtslehre aus.

Zustimmung

- Die Stärkung der Einwilligung führt zu einem Kommunikations- und Kooperationsverhältnis zwischen Datenverarbeiter und Betroffenem und kann die Handlungsfähigkeit des Betroffenen – durch eine bessere Information – stärken.
- Es besteht ein enger Zusammenhang zwischen dem Erfordernis der Zustimmung und einer gesellschaftlicher Kommunikation über Datenschutz, Denn in diesem Fall müssen die Datenverarbeiter informieren, legitimieren und um Vertrauen werben.
- Datenschutzrecht muss die Position des Schwächeren schützen. Dies ist auch bei einer Stärkung der Zustimmung und ihrer Freiwilligkeit zu berücksichtigen.
- Im Arbeitsrecht ist die Freiwilligkeit der Zustimmung nur sehr bedingt gegeben. Der AN hat keine realistische Möglichkeit die Einwilligung zu verweigern. Die Wirksamkeit des Instruments im Arbeitsverhältnis ist daher fraglich. Es muss verhindert werden, dass der Arbeitgeber in diesem Bereich eine noch größere Machtposition erlangt. (s.u.)
- Freiwilligkeit der Zustimmung(sverweigerung) darf nicht zu höheren Kosten führen. (Bsp.: kontoungebundene GeldKarte, Guthabenkonto)
- Datensparsame Basisdienstleistungen (z.B. TK, Post) sollten wettbewerbsneutral definiert werden. Dazu treten dann zusätzliche Dienstleistungen.
- Man könnte gesetzlich vorsehen, dass es zur allgemein vorgesehenen Datenverarbeitung auch noch eine Alternative ohne Personenbezug geben muss (preisneutral).
- In die Kostengestaltung der Datenverarbeitung wird man gesetzlich nicht eingreifen können. Wäre eine Formulierung „keine Nachteile“ ähnlich dem SächsDSG eine Lösung?
- Bei einer Formulierung „rechtlich anerkannte Interessen“ wäre eine Verarbeitung zu Marketingzwecken möglicherweise ausgeschlossen.
- Bei „rechtlichem Interesse“ als Maßstab bekommt man aber Probleme mit dem Outsourcing der Datenverarbeitung, soweit diese mehr ist als Datenverarbeitung im Auftrag. Denn die mit ihr verbundene Übermittlung mag wirtschaftlich notwendig sein, erfüllt aber kein rechtliches Interesse.
- Die Zustimmung muss das „berechtigte Interesse“ als Zulässigkeitsvoraussetzung einer Datenverarbeitung ersetzen. Das gegenläufige Interesse des Betroffenen ist immer berührt, wenn er hätte gefragt werden können (weil seine Selbstbestimmung ignoriert worden ist).
- Die Beweislast, dass eine Zustimmung erfolgte und in welchem Umfang muss beim Datenverarbeiter liegen. Ihm kommt auch die Benachrichtigungspflicht zu und er muss nachweisen, dass er richtig und vollständig (auch über den Empfänger) informiert hat.
- Man könnte die Anforderung spezifisch für die einzelnen Verarbeitungsphasen (Erhebung, Zweckänderung, Übermittlung etc.) abschichten.

- Außerhalb der Vertragsabwicklung bedürfen Übermittlungen immer der Zustimmung.
- Außer in den genannten Fällen (Delikt) ist ein gesetzlicher Erlaubnistatbestand auch etwa bei einer DV durch Rechtsanwälte (Daten des Prozessgegners) notwendig.
- Die drei für die Wirtschaft interessanten Zweckänderungen sollten folgendermaßen geregelt sein:
  - Marketing: Opt-in,
  - Risikoabwägung vor Vertragsschluss: nur mit Zustimmung möglich,
  - Abwicklung von notleidenden Verträgen: „rechtliches Interesse". Diese Informationen sind auch für andere Vertragspartner des Kreditnehmers interessant. Doch für Auskünfte an diese müssen die spezifischen Risiken berücksichtigt werden (daher nur bei Verhältnismäßigkeit (nicht in Bagatellfällen) und nur bei Nachweise des Interesses an der Abfrage), allerdings auch Probleme öffentlicher Verzeichnisse berücksichtigen.
- AGB-Kontrollen von Formularzustimmungen müssen mit einer grundlegenden Änderung der Kontrollpraxis der Aufsichtsbehörden, insbesondere mit einer ausreichenden personellen Ausstattung einhergehen.

Datenverarbeitung mit ungezieltem Personenbezug

- Es sollte ein anderer Terminus gefunden werden, der jetzige suggeriert, dass diese Daten aus dem allgemeinen Datenschutz herausgenommen werden, was nach dem Volkszählungsurteil – „keine belanglosen Daten" – problematisch sein dürfte. Kritisch ist v.a. der Zeitpunkt, an dem ungezielte zur gezielten DV umschlägt.
- Klarstellung: Datenverarbeitung mit ungezieltem Personenbezug ist nur unter spezifischen Anforderungen möglich. Die Unterscheidung ist notwendig und sinnvoll, da es nicht gelingen wird, alle Formen der DV gleichen Anforderungen zu unterwerfen.
- Die notwendige frühzeitige Löschung bei ungezieltem Personenbezug ist eine Verbesserung des Datenschutzes.
- Beispiele für die Verwendung des Terminus:
  - BVerfGE 100, 366, kein Eingriff,
  - Simitis/Damann, Kommentar zu Art. 8 der europ. DSRL zu sensitiven Daten.
- Rein technisch bedingte DV könnte unter diese Kategorie „ohne gezielten Personenbezug" fallen, wenn die Daten sofort danach gelöscht werden, ansonsten ist es immer gezielte Verarbeitung personenbezogener Daten.
- Zur ungezielten DV könnten solche Prozesse zählen, bei denen die Daten im Anschluss an deren Verwendung nur deshalb gespeichert würden, damit ein Auskunftsanspruch befriedigt werden kann. Dieser zusätzliche Anfall von Daten kann nicht gewollt sein.
- Ziel ist es, das TK-Recht in das BDSG zu integrieren, so dass bisherige gesonderte Bestimmungen des TK-Recht in das BDSG einfließen müssen.
- Ein BDSG, welches das TK-Recht integriert, darf nicht hinter dessen Schutzniveau zurückfallen.
- Bei Einführung verschiedener Kategorien der DV besteht die Gefahr der Unschärfe, Verwirrung und Scheinsystematik.
- Wer bestimmt die Zielrichtung der Datenverarbeitung?
- Das BVerfG unterscheidet bei den Anforderungen an die DV nach Erfassen und Speichern.
- Besser als zwischen ungezielter und gezielter Datenverarbeitung zu unterscheiden wäre es, von einer konkreten Zweckdefinition auszugehen (§ 31 BDSG) und dafür besondere Regelungen vorzusehen.

- Möglicherweise sollte die Kategorie „ungezielte DV“ aufgegeben werden. Dies hätte den Vorteil, eine differenziertere fallbezogene Güterabwägung vornehmen zu können.
- Wenn, wie von den Gutachtern intendiert, die Kategorie ungezielte DV durch striktere Zweckbindung und eine sofortige Löschung einen höheren Schutz bietet, so ist sie jedenfalls erwägenswert. Man sollte eine Definition wagen.
- Für Bedarfsträger gelten keine Unterschiede. Sie haben bei gezielter und ungezielter DV die gleiche Kompetenzen.
- Man sollte sich nicht der Illusion hingeben, dass die Bedarfsträger nicht über die Mechanismen des Straf(prozess)rechts Zugriff auch auf Daten der ungezielten DV zugreifen werden.

Maßnahmen der IT-Sicherheit

- Motiv für Löschung von Daten hat sich verändert, früher war es eine Frage der Kosten von Speicherkapazität, heute spielen Kosten keine Rolle, also wird alles gespeichert.
- Pseudonymisierung muss für die Nutzer attraktiv werden (Spaßfaktor).
- Datenschutztechnik kann gebaut werden, aber scheitert es daran,
  - dass diese von den Menschen nicht angenommen wird und nur als eine Idee von einer kleinen Gruppe zur Beglückung der Menschheit angesehen wird,
  - dass die Datenschutzbeauftragten zur Kontrolle der DV gar nicht mehr in der Lage sind,
  - dass es an der zusätzlichen Beratung zur sinnvollen Nutzung der Datenverarbeitung mangelt?
- Ist ein Recht auf Anonymität und Verschlüsselung durchsetzbar?
- Für die Zielkategorien kann § 10 DSG-NRW als Vorbild dienen.
- Gütesiegel und Datenschutzaudit sind brauchbare Instrumente.
- An eine Änderung des Vergaberechts, welches dann neben der Wirtschaftlichkeit auch die Datenschutzfreundlichkeit eines Angebots berücksichtigt, wäre zu denken.
- Die *Priorisierung* der Maßnahmen muss normativ gefordert werden.
- Der *Selbstschutz* muss erlaubt, die Autonomie des Nutzers technisch abgesichert sein.
- *Open source* muss gefordert werden. Hier sollten aber Übergangsfristen vorgesehen werden.
- Datenschutzfreundlichen Tools müssen aber erlaubt sein. Etwaige Kollisionen mit intellectual property rights könnten in einem gesonderten Paragrafen im BDSG berücksichtigt werden. (in USA, sind Dekompilierung und Mittel, mit denen Quellcodes erkannt werden können, u.a. aus urheberrechtlichen Gründen verboten.)
- Alte Begriffe (z.B. § 9) sollten nicht ohne Grund ad acta gelegt werden, sondern mit neuen, die sich einfügen können, verbunden werden.
- Der Vorrang des Datenschutzes vor Performance muss als generelles Ziel definiert werden. Dies ist besser als die schwammige Formulierung „angemessen“, die in der Praxis immer zu Problemen führt, da dann die Frage im Raum steht: „Was können / wollen wir uns wirtschaftlich leisten“.
- Daneben müssen auch am „state of the art“ ausgerichtete speziellere Ziele festgeschrieben werden, selbst auf die Gefahr hin, dass sie veralten (z.B. Verschlüsselung bei Übermittlung über öff. Leitungen, Jedes Email-Programm mit Verschlüsselungsfunktion).
- Wie kann sichergestellt werden, dass der Stand der Technik immer die Grundlage der Anforderungen an die IT-Sicherheit ist – wie soll man diese Forderung prozeduralisieren: über Institutionen wie BSI, LfDs?

- Schlecht wäre es, wenn hier eine Vereinheitlichung erfolgt, die Konkurrenz ausschließt. Dann sollte man auf Institutionalisierung verzichten.
- Die Auslegung des bisherigen § 9 BDSG birgt durch den Bezug auf die Verhältnismäßigkeit große Probleme für bDSB, da immer die eigenen Interessen des Unternehmens berücksichtigt werden. Deshalb sollten solche Formulierungen weggelassen werden.
- Statt der bisherigen 10 Gebote sind vier Schutzziele der IT-Sicherheit ausreichend, praktikabel und langfristig nutzbar (s. Papier des BvD). Formulierungen in der Sprache der Informatik anstreben.
- Was bedeutet Vertraulichkeit – nur Schutz ggü. Dritten oder auch ggü. Kommunikationspartner? Hier sollte begrifflich unterschieden werden zwischen Schutz von Inhalten (Vertraulichkeit) und Schutz der Identität (Anonymität).
- IT-Sicherheit und Datenschutz sind nicht deckungsgleich, vielmehr ist die IT-Sicherheit nur ein Hilfsmittel für den Datenschutz, Anonymität ist Ziel des Datenschutzes, nicht der IT-Sicherheit.

Marktmechanismen

- Das Herausgabeverlangen eines ökonomischen Vorteils bei Verletzung von Datenschutzregeln sollte im Wege einer Klage ermöglicht werden - wie im Bereicherungsrecht.
- Ähnliches gilt für das Urheberrecht bei illegaler Verwertung und für das Deliktsrecht (Soraya-E). Unrechtsgewinnabschöpfungen gibt es auch im Strafrecht. Parallelen zum Ausgleich für illegale Verwertung hier fruchtbar machen.
- Verbandsklagen zur Geltendmachung eines Kollektivschadens wären wünschenswert. Eine rechtsvergleichende Untersuchung von Hopt u.a. zu Verbandsklagen im Schadensersatzrecht sollte berücksichtigt werden.
- Bereits bestehende Abschöpfungsmaßnahmen des OWi-Rechts sollten mehr genutzt werden (§17 Abs. 4 OWiG)
- Wer keinen Datenschutzbeauftragten bestellt, zahlt heute schon Bußgeld – Höhe ist allerdings fragwürdig

Selbstregulierung

- Selbstregulierung ist wichtig, wenn behördliche Aufsichtsmechanismen nicht wirken. Allerdings besteht die Gefahr von Kartellen – siehe Formularzustimmungen einer ganzen Branche. Hier sind entsprechende Kontrollen notwendig.
- Dem Demokratiedefizit der Selbstregulierung muss durch gesetzliche Regulierungen der Grundsätze Rechnung getragen werden. Dies kann durch staatliche Anerkennung von Maßnahmen der Selbstregulierung und durch die Beteiligung von Verbänden mit gegenläufigen Interessen geschehen. Insoweit wäre auch eine Anerkennung von Verbänden wie in § 22a AGBG und die zwingende Beteiligung von Verbraucherverbänden anzustreben.
- Kontrollinstrumentarien müssen Bestandteil des Gesamtinstituts Selbstregulierung sein, sowohl intern als auch extern (Aufsicht, Bericht).
- Wie kann die Verbindlichkeit von Regelungen hergestellt werden, um nicht zuletzt auch „Trittbrettfahrer“ zu vermeiden?
- Exekutive Allgemeinverbindlichkeitserklärungen wie bei Tarifverträgen oder Verordnungen wären zu erwägen.
- Verbandsklagerecht sollte Verbraucherverbänden und bspw. BvD, DvD eingeräumt werden. Klagebefugnis würde bspw. DvD allein überfordern. Finanzielle Kompensation wäre nötig – Lizensierung von Prozessbeteilgten.
- Gerichtliche Kontrolldichte könnte dann zurückgenommen werden, wenn die „Richtigen“ an der Entscheidung teilgenommen haben (vgl. Prüfungsentscheidung, § 1 KSchG).

- Sorge, dass nach Zustimmung von Standard-AGB die Kontrolle durch Aufsichtsbehörden aufhört – wie die Erfahrungen belegen.
- Ein Ausführungsgesetz zum Datenschutzaudit könnte im Vorgriff auf die zweite Stufe der BDSG-Novellierung verabschiedet werden. Dabei könnte auf einen Entwurf von Prof. Roßnagel aus dem Jahr 1999 zurückgegriffen werden, der sich auf acht Paragrafen und einen Anhang beschränkt.

Arbeitnehmerdatenschutz

- Angesichts des ungleichen Kräfteverhältnisses im Arbeitsrecht muss die Einwilligung besonders gestaltet sein: entweder ganz ausschließen oder aber verschärfte Anforderungen.
- Im Arbeitsverhältnis widerstreiten das Interesse des Arbeitgebers, alle Daten zu erlangen und das Recht des Arbeitnehmers auf individuelle Datensicherungsmaßnahmen (persönliche Kommunikation auch im Arbeitsverhältnis, Grundrechte, Recht am eigenen Schreibtisch, Entwurfsordner, Zettelkasten).
- BVerfG hat den Schutz der Persönlichkeitsrechte (Fernmeldegeheimnis) auch für den Arbeitsplatz bestätigt. Für den Emailverkehr bedeutet diese, dass wenn die Email ein Telefonat ersetzt, diese geschützt ist, wenn sie aber ein Schriftstück ersetzt, der Schutz nicht greift.
- Die Rechtsumsetzung ist problematisch, denn das Fernmeldegeheimnis gilt ohnehin sowohl im privaten Bereich als auch im Arbeitsverhältnis, unterscheidet nicht zwischen Arbeitnehmer und Privatperson.
- Verschlüsselte Daten könnten dem Unternehmen über den bDSB zugänglich gemacht werden, der als eine Art Vorabkontrolle die Daten auf deren Geschäftsrelevanz prüft.
- BAG betont das Mitbestimmungsrecht auch in der Datenverarbeitung. Dies sollte auch bei der Unterteilung in gezielte und ungezielte DV beachtet werden (Rückwirkung auf die Anwendung des § 87 Nr. 6 BetrVG).
- In welche Kategorie (ung./gez.) fällt die Suche mit unternehmensinternen Suchmaschinen? Wo beginnt der Personenbezug – z.B.: anonyme Statistik führt zur Kündigung aller über 55-jährigen.
- Es ist zu bedauern, dass der Düsseldorfer Kreis festgestellt hat, dass § 85 TKG nicht für Arbeitnehmer gilt. Siehe dagegen die Begründung zu § 85 TKG.

Betriebliche Datenschutzbeauftragte (bDSB)

- Datenschutzniveau hängt von der Umsetzung im Betrieb ab.
- Viele bDSB erfüllen eine Alibifunktion. Dies ist nicht zuletzt der unzureichenden Aufsicht geschuldet (BW: 4 ½ Stellen für 600.000 Unternehmen). Auch ärztliche Praxen müssten DSB bestellen.
- Fachkunde und Zuverlässigkeit müssen definiert werden (vgl. Formulierungsvorschlag zu § 4 f des BvD).
- Im betrieblichen Datenschutz bedarf es sowohl hinsichtlich der Betriebsräte als auch hinsichtlich der betrieblichen Datenschutzbeauftragten einer umfangreichen Qualifikation.
- Externe DSB werden in größeren Unternehmen immer beliebter. Aus den Verträgen ergeben sich häufig ¼-jährliche Kündigungsfristen.
- Kleinere Unternehmen meinen, sich einen externen DSB nicht leisten zu können.Es wäre sinnvoll, wenn kleinere Unternehmen externe DSB (gemeinsam) beauftragten – z.B. alle Ärzte eines Gebietes einen DSB.
- Beauftragung juristischer Personen ist abzulehnen, da dabei der Kündigungsschutz umgangen werden kann und nur eine unverbindliche namentliche Beauftragung erfolgt.

- Für die bDSB könnten ähnliche Regelungen wie für Betriebsärzte gefunden werden, Quotelung der Arbeitszeit entsprechend der Betriebsgröße. (ArbG Darmstadt) Anforderungen müssen verbindlich sein: Mitarbeiterzahl, Ressourcen allgemeiner Art. Orientierung am Umweltschutzbeauftragten?
- Aufgrund der zu berücksichtigenden Ausrichtung der Unternehmen wird es dafür keine praktikable Formel geben.
- Die zwangsweise Bestellung eines Vollzeit-DSB ist problematisch, da dadurch der Datenschutz ein Zwangsimage erhält, welches kontraproduktiv ist (so aber noch im Bündnis 90/Die Grünen-Entwurf).
- Bei Teilzeit-DSB bezieht sich der Kündigungsschutz nur auf den jeweiligen Anteil, so dass es trotzdem zu einer Kündigung kommen kann. Kündigungsschutz für bDSB wie für Betriebsräte.
- Dem Anrufungsrecht des bDSB gegenüber den Aufsichtsbehörden muss der derzeitige Zündstoff genommen werden, wenn bspw. die Anrufung durch den bDSB zu Bußgeldern für das Unternehmen führt. Die Aufsichtsbehörde ist Kontroll- und Beratungsstelle in einem! Eine Pflicht zur Anrufung festschreiben?
- Anlehnung an Steuerrecht? Selbstanzeige führt zu Straffreiheit, wenn Missstände beseitigt werden?
- Das Verhältnis zum und die Kooperation mit dem Betriebsrat müssen geregelt werden. Dabei müssen die beidseitigen Interessen berücksichtigt werden (Unabhängigkeit vs. Mitbestimmung auch bei Maßnahmen der DV). Bei Überschneidungen der Aufgaben und Interessen können wünschenswerte Synergien (Durchsetzungsmöglichkeiten des Betriebsrates) entstehen.
- Die Kontrolltätigkeit des bDSB muss sich auch auf die DV des Betriebsrates erstrecken. Beanstandungen und Berichtspflicht sollte aber nicht gegenüber der Betriebsleitung sondern gegenüber dem Vorsitzenden des Betriebsrates erfolgen.
- Die wichtigste Fachkunde, die ein bDSB besitzen muss, ist die genaue Kenntnis der Datenverarbeitung im Unternehmen. Alles andere ist zweitrangig.

4.4 Workshop mit Mitarbeitern des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 2. April 2001 in Bonn

Rolle des BSI im bisherigen und künftigen Datenschutzsystem

- Der Auftrag des BSI bezieht sich auf die Unterstützung von Behörden bei der Einrichtung sicherer Technik, nicht auf die Aufrechterhaltung der inneren Sicherheit. Berührungspunkte gibt es allenfalls bei der Unterstützung des BfV, BKA und anderer Dienste.
- In der bisherigen Praxis entsteht in konkreten Fällen bisweilen ein Interessenkonflikt durch eine Doppelfunktion des BSI als Berater des BfD und als Berater einer Institution im Rahmen einer Kontrolle durch den BfD. Die Beratungsfunktion für den BfD hat allerdings Priorität.
- Ob künftig auch weitergehende Aufgaben durch das BSI erfüllt werden sollen, hängt vom politischen Willen ab. Für Fragen der Verschlüsselung ist Grundlage der Kabinettsbeschluss zur Förderung der Sicherheit in der IT-Technik vom Juni 1999.
- Das BSI könnte künftig als Kompetenzzentrum beratende Funktion gegenüber BfD und LfD erhalten, ggf. auch im Rahmen der Zertifizierung datenschutzfreundlicher Technik.
- Könnte man ein gemeinsames Forschungsinstitut der LfD und des BfD einrichten?
- Könnte es einen „know-how-Verbund“ von BSI, LfD, BfD, Privatwirtschaft geben?

Zweckbindung

- Die Zweckbindung kann durch eine konsequente Rechteverwaltung (Identifizierung der Institution, die Zugriff auf die Daten haben soll) erreicht werden. In offenen Systemen helfen im Grunde nur elektronische Wasserzeichen.
- *Replik:* Wasserzeichen sind eigentlich unzureichend, da sie nur zu einer nachträglichen Feststellung der unzulässigen DV dienen können. Daher ist eigentlich nur ein physischer Schutz der Zweckbindung möglich.
- Bei kleinen Datensätzen wird die Verbindung mit einem Wasserzeichen noch problematischer. Wie soll darin ein Wasserzeichen versteckt werden?
- Das Datum müsste mit dem Zweck verbunden werden. Allerdings ist die unauflösliche Verbindung des Datums mit der Kennzeichnung des Zwecks wie auch die Frage der klassifizierten Daten angesichts der Änderungsmöglichkeiten bis heute ein ungelöstes Problem. Eine diesbezügliche Forderung aufzustellen, hat daher auch wenig Sinn. Solange muss auf die Kryptierung mit einer entsprechenden Schlüsselverwaltung zurückgegriffen werden, wenngleich dies insbesondere im Bezug auf offene Systeme kein „Allheilmittel" ist.
- Im Sinne des Datenschutzes soll die unzulässige Datenverarbeitung von vornherein verhindert werden. Insoweit sind Möglichkeiten im Bereich des Copyright, die eine nachträgliche Kompensation ungenehmigter Nutzungen sicherstellen, nicht effektiv.
- *Replik:* Die Möglichkeit einer nachträglichen Feststellung von Verletzungen des Datenschutzrechts wäre schon ein Fortschritt, wenn sie mit rechtlichen Maßnahmen verbunden würde.
- Bei Tamperresistance gibt es einen ständigen Wettlauf mit den Angreifern (Beispiel Chipkarte). Die Chancen sind gleichwohl groß, da jeder Angriff zu neuen Schutzmaßnahmen führt.
- Tamperresistant Systems betreffen v.a. die Hardware. Ein ständiges Update kostet viel Geld. Eine Massennutzung ist zwar als „Datenschutzparadies" wünschenswert, jedoch unrealistisch. Man muss sich vor „Datenschutzterror" hüten. Wer sollte die hohen Kosten tragen.
- Die Hardware könnte den Zweck kontrollieren, der vom Systemherrn in Form von Rollen vorgegeben wird. Eine Übertragung in andere Rollen ist dann nicht möglich. Der entscheidende Punkt ist dabei die Rollendefinition. Deren Änderung könnte von einer Zulassung der Kontrollbehörde abhängig gemacht werden.
- Ein Beispiel für eine notwendige Zweckbindung sind Lokalisationsdaten. Wie kann der Anbieter dazu gezwungen werden, Daten nur für den zulässigen Zweck zu benutzen. Kann man in diesem Sinne ein System abdichten?

§ 9 BDSG

- Die Anlage zu § 9 BDSG bedient sich bisher einer altmodischen Sprache und sollte – soweit diese Form beibehalten wird – aus Sicht der IT-Sicherheit geschrieben werden, kompakter sein und die Maßnahmen so konkret beschreiben, wie man sie haben will.
- Die Ziele sollten im Vordergrund stehen, Maßnahmen können definiert werden, die Anforderungen ergeben sich bereits aus der Beschreibung der Schutzziele heraus.
- Unterschiedliche Schutzstufen sind sinnvoll, bspw. eine für Adressdaten und eine andere für medizinische Daten.
- Es bedarf eines maßgeschneiderten Schutzniveaus für jede Anwendung. Für jede Anwendung sollte noch besser ein eigene Protection Profile formuliert werden.
- Einzelne Daten erhalten ihre Sensitivität häufig erst durch die konkrete Nutzung. Daher ist ein einheitliches hohes Schutzniveau sinnvoll, zumal die Kosten für hohe Sicherheitstech-

nik nicht bei der einzelnen Anwendung, sondern bei der Anschaffung und Einrichtung von Systemen entstehen. Diese können dann für alle Anwendungen genutzt werden.

- Das BMVg arbeitet mit einem gestuften Schutzkonzept für die Verarbeitung personenbezogener Daten. Ebenso existiert seit fünf Jahren ein Schutzstufenkonzept beim LfD im Saarland.
- Verschiedene Schutzanforderungen erleichtern das Leben (Kosten, Aufwand)! Es lässt sich leichter entscheiden, welche Anforderungen im Einzelfall zu stellen sind. Auch ist es nicht mehr notwendig, in jedem Einzelfall eine Verhältnismäßigkeitsprüfung durchzuführen.
- Zu hohe Anforderungen können die Akzeptanz des Datenschutzes mindern.
- Stufung ist sinnvoll, wenn bestimmte Verfahren nicht flächendeckend angewendet werden können, z.B. Kryptographie wegen der Inkompatibilität verschiedener Systeme. Stufung ermöglicht eher, einen starken Schutz für höhere Stufen durchzusetzen.

Profiles

- Dies ist ein sinnvoller Ansatz z.B. für Pseudonymisierungsverfahren oder Statistiken im medizinischen Bereich. Wer trägt allerdings die Kosten der Entwicklung der Profiles? Welche Institution sollte die dahingehende Entwicklung anstoßen?
- Entwicklungen könnten in Zusammenarbeit von LfDs, BfD und Universitäten, bspw. im Rahmen von Diplomarbeiten, erfolgen. Es könnten auch staatliche Vorleistungen, ggf. mit Rückzahlungsklauseln für den Fall des kommerziellen Erfolges in Erwägung gezogen werden.
- Bisher haben nur Hersteller Protection Files entwickelt, z.B. hat Oracle zwei Profiles für Datenbanken entwickelt (die nur Oracle-Produkte erfüllen).
- Der Anstoß für die Entwicklung von Profiles sollte auch künftig von Herstellern kommen. Beim BSI besteht kein Interesse, einzelne Hersteller zu unterstützen. Das BSI ist als Initiativinstitution auch nicht geeignet. Möglicherweise kämen die LfDs oder der BfD dafür in Frage, die die Anforderungen an Profiles kennen und für eine Hersteller-neutrale Entwicklung sorgen könnten.
- Die Rolle des BSI beschränkt sich derzeit auf die Unterstützung von (potentiellen) Anwendergruppen bei der Formulierung von Profile-Anforderungen. Der Aufwand für die Entwicklung ist relativ groß, z.B. Bankenbereich (Schätzung):
  - Arbeitsgruppe mit ca. 5 Fachleuten, die das Anwendungsfeld beschreibt (10 Sitzungen)
  - Hinzuziehung externer Experten, die die Ziele in Protection Files einbringen (1 Mann-Jahr).
  - Prüfung auf Praxistauglichkeit (ca. 2 Monate).
- Es wird empfohlen, dass das BMWi, Profiles erarbeiten lässt.

Verhältnis BSI – BfD

- Zur Zeit bezieht sich Beratung nur auf den BfD, in etwa fünf Fällen pro Jahr (ca. ein Mannjahr). Die Tätigkeit war rückläufig, da der BfD in den letzten Jahren auch eigene Techniker (inzwischen etwa 20) und nicht nur Juristen beschäftigt. Die zunehmende eigene Beratung durch die Techniker des BfD wird begrüßt. Bei neuen Projekten von übergeordneter Bedeutung und kompakter Fragestellung (z.B. Einführung einer neuen Geldkarte) ist die Einbeziehung des BSI sinnvoll.
- Die Anfragen beziehen sich auf allgemeine Probleme (bspw. Verschlüsselungsprogramme) oder auf konkrete Prüfungen und Kontrollverfahren des BfD.
- Die Auflage des BfD kann auch eine Sicherheitsanalyse des BSI beinhalten.

- Beratungsfunktion könnte auch auf die LfD ausgeweitet werden, soweit dies politisch gewollt ist und die nötigen Kapazitäten im BSI vorgesehen werden (angesichts der Bund-Länder-Kompetenzen und -Interessen allerdings fraglich).
- BSI würde auch die explizite Erwähnung seiner Beratungsfunktion im BDSG begrüßen

Zertifizierung - Evaluierung

- Die Mängel der bisherigen Zertifizierung sind bekannt:
  - Das Ob, die Prüfkriterien und die Prüftiefe liegen in der Hand der Hersteller.
  - Die Zertifizierung basiert insofern auf dem Zufälligkeitsprinzip.
- Lediglich bei Lesegeräten für Krankenversicherungskarten gab es die Verpflichtung zur Zertifizierung und die Mindestanforderungen an die Prüfung nach „E2 mittel“. Die Zertifizierung hat angesichts der relativ geringen Anforderungen an die Prüfung zu keiner Erhöhung der Kosten für die Lesegeräte geführt.
- Eine Verpflichtung zur Zertifizierung wird notwendig sein, wenn die Anforderungen durch Protection Profiles vorgegeben werden (sollen). Sie muss im Zusammenhang mit den Protection Files der Anwender gesehen werden, ansonsten ist sie nicht aussagekräftig.
- Mit der Vorschrift zur Zertifizierung wurden im Rahmen des SigG schlechte Erfahrungen gemacht. Wenn die zwingende Zertifizierung vorgesehen werden soll, dann muss genau beschrieben werden, wie diese aussehen muss. Dies ist aber in einem Gesetz in der notwendig spezifizierten Form kaum möglich.
- Es gibt aber funktionierende Verfahren im Umweltbereich.
- Für die Zertifizierung in Realzeit könnte auch ein gestuftes Prüfverfahren dienlich sein, in welchem nach vier Wochen eine vorläufige, mehr oberflächliche Prüfung erfolgt ist und zu einem späteren Zeitpunkt das tiefere Prüfergebnis vorgelegt wird.
- Die Zertifizierung könnte mit der Vorabkontrolle verbunden werden. Die erfolgte Prüfung für die Zertifizierung (die von den Kontrollstellen nicht zu leisten wäre) würde die Vorabkontrolle vereinfachen.
- Der heutige Zeitverzug bei der Zertifizierung liegt daran, dass die Vertriebsabteilung diese als verkaufsfördernd ansieht und für das derzeit zu verkaufende Produkt einholt und nicht bereits die Entwicklungsabteilung. Wäre ein Zertifikat von vornherein gesetzlich gefordert, so müsste bereits der Entwicklungsbereich eines Unternehmens diese in seine Planung integrieren.
- Bei einer Zertifizierung ohne die Unterstützung der Hersteller ergeben sich Probleme:
  - Informationen fehlen – z.B. source code und Nachweis vertrauenswürdiger Entwicklungsumgebung,
  - kein Einblick in die Vorgaben / Dokumentation der Entwicklung, Schon bei der Entwicklung muss eine korrekte Dokumentation erfolgen,
  - aufgetretene / gefundene Fehler können nicht behoben werden.
- Es ist Aufgabe des Gesetzgebers, wenn bestimmte Techniken gewollt sind, diese zu definieren.
- Es ist möglich (bspw. aus Linux) einen Kern mit speziellen Anwendungsfunktionen herauszunehmen und diesen gesondert zu zertifizieren.
- Nicht an alle Systeme und Anwendungen sollten die gleichen hohen Anforderungen gestellt werden. Zwänge sind aber in einzelnen Fallgruppen sinnvoll, z.B. die Forderung nach Sicherheitsanalysen bei Herstellern spezieller Anwendungen (z.B. SAP, Human Ressources).

- Dafür könnten konkrete Produktklassen entwickelt werden. Deren Einführung kann zu einem geringeren Aufwand der Prüfung führen, da Evaluatoren Erfahrungen im speziellen Bereich entwickeln würden. Z.B. konnten die Evaluatoren den Aufwand für die Krankenversicherungs-Chipkarten auf 1/10 senken.

Durchsetzung des Standes der Technik

- Das BSI wird in diesem Bereich nur unverbindliche Aussagen treffen können, allenfalls innerhalb von Behörden wird an eine Verbindlichkeit zu denken sein. Ansonsten werden Aussagen des BSI zum *state of the art* nur als Empfehlungen ergehen können.
- Die Einhaltung gesetzlicher Auflagen und der vom BSI vorgegeben Anforderungen könnten als Vermutungsregel für eine ordnungsgemäße DV dienen.
- Das BSI bietet ein Gütesiegel für die Einhaltung der Anforderungen des Grundschutzhandbuchs an. Dies ist viel weniger verbindlich als Zertifizierungen und könnte ein Weg sein, bestimmte Anforderungen schneller durchzusetzen.
- Ein Gremium, das den gesammelten Sachverstand in diesem Bereich vereint (das BSI dabei einbinden würde), könnte Akzeptanz und Klarheit bringen.
- Solche klaren Aussagen würden von betrieblichen DSB angenommen, weil handhabbar.

Abstrahlsicherheit

- Die Abstrahlsicherheit muss sich nach der Sensitivität der verarbeiteten Daten richten – insoweit ein abgestuftes Verfahren. Eine gesetzlich geforderte absolute Abstrahlsicherheit bei jeder Datenverarbeitung aus Gründen des Datenschutzes ist nicht vorstellbar, auch nicht nötig und wäre i.ü. überzogen.
- Völlige Sicherheit wird im streng geheimen Bereich erforderlich sein, ansonsten reichen räumliche Überlegungen (Platzierung des PC nicht am Fenster, Mauerdicke etc.) aus.

Löschung

- Für die „normale“ Löschung ist ein dreimaliges Überschreiben mit wechselnder bit-Folge ausreichend. Dafür existieren bereits Programme, die dies ohne großen Zeitaufwand problemlos ermöglichen.
- Für besonders sensitive Daten gehen die Anforderungen hin bis zur physischen Vernichtung. (Es gibt eine BSI-Publikation „Löschen für den höheren Schutzbedarf“.)
- Beim Überschreiben muss auf die verschiedenen Spurbreiten geachtet werden.
- Dokumente dürfen keine zusätzlichen Informationen (versteckte Kanäle) enthalten von deren Existenz der Ersteller oder Übermittler keine Kenntnis hat.
- Im BDSG könnte auf das Grundschutzhandbuch des BSI Bezug genommen werden.

Biometrie

- Die Entwicklung und Nutzung ist bereits in vollem Gange. Biometrische Erkennung wird nicht mehr wahrgenommen und wird auch nicht mitgeteilt werden.
- Das Hauptproblem der Biometrie ist, dass sie nicht verändert werden kann, d.h. wenn die entsprechenden Daten einmal bekannt sind, besteht kein Schutz mehr. Es ist daher fraglich, ob sie für alle Authentifizierungen wirklich die sichere Lösung ist, wenngleich sie gegenüber PIN (Merkfähigkeit, Ausspähungsmöglichkeit) einen deutlichen Fortschritt darstellt.

Betriebliche Datenschutzbeauftragte

- Der Mindestzeitrahmen für die Tätigkeit eines betrieblichen DSB sollte gesetzlich normiert sein.

4.5 Workshop mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2001 in Düsseldorf

Grundstruktur

- Die **Konzentration grundsätzlicher Regelungen im BDSG** wird begrüßt, da bisherige bereichsspezifische Regelungen oft scheinpräzise sind, weil bei Lücken unklar ist, was dann gilt. Sowohl für die Verwaltung als auch für den Betroffenen wäre eine solche Konzentration eine willkommene Vereinfachung.
- Bei einer Konzentration darf aber der Grund der bereichsspezifischen Regelungen nicht außer Acht gelassen werden: der Sachbearbeiter, der nur sein Fachgesetz kennt. Durch saubere Verweisungstechnik kann die Aufgabe der bereichsspezifischen Regelungen kompensiert werden und das Datenschutzrecht handhabbar gemacht werden.
- Die Vereinheitlichung des Datenschutzrechts darf aber nicht zum Absenken des Datenschutzniveaus führen.
- Die Notwendigkeit einer Vereinheitlichung und damit der Einbeziehung der TK, Teledienste und herkömmlicher Datenverarbeitung ergibt sich schon daraus, dass diese wegen der fortschreitenden Vernetzung immer schwerer voneinander zu trennen sind. Daher ist die Zusammenführung dieser Bereiche in einem Gesetz auch sinnvoll und gewollt.
- Ein künftiges BDSG könnte sich an der Struktur des UGB – Allgemeiner Teil ./. Besonderer Teil – orientieren.
- Es bestehen allerdings Bedenken, dass ein derart komplexes Recht von den einzelnen Sachbearbeitern zu bewältigen ist.
- Das Gutachten sollte auch Aussagen zu den Chancen und Möglichkeiten, die Anzahl bereichsspezifischer Gesetze zu verringern, enthalten.
- Die **Grundsätze einer rechtmäßigen DV** müssen präzise beschrieben werden, auf offene Abwägungsklauseln sollte verzichtet werden.
- Bei der Zulässigkeit der DV muss auch in Zukunft zwischen **öffentlichem und privatem Bereich** unterschieden werden. Dies gilt sowohl für die Frage der Zustimmung (im öff. Bereich wird oft darauf zu verzichten sein), als auch für Transparenz, Zweckbindung und Erforderlichkeit. Allerdings können Rahmenbedingungen und generelle Restriktionen der DV für beide Bereiche vordefiniert sein.
- Die unterschiedlichen Anforderungen an den Datenschutz im öffentlichen und privaten Bereich ergeben sich bereits aus der grundrechtlichen Verankerung desselben. Im öffentlichen Bereich bedarf es immer einer speziellen Rechtsgrundlage zur DV. Oft reichen aber allgemeine Regelungen der Aufgabenstellung aus (z.B. im Wasserrecht, LuftVG, Schulgesetze, Universitätsgesetze, in Berlin: Oper, Friedhof).
- Für die Zweckbindung muss folgendes gelten:
  - · im öffentlichen Bereich gibt es gesetzlich normierte DV-Tatbestände,
  - · im privaten Bereich die ausdrückliche Zustimmung bzw. den Vertrag.
- Das Gesetz sollte so gegliedert sein, dass zuerst die Datenverarbeitung erlaubt wird (hierfür enumerative Erlaubnisnormen beibehalten) und dann sollten die Schranken der grundsätzlich zulässigen Datenverarbeitung geregelt werden. Zu diesen - für den öffentlichen und privaten Bereich gemeinsam fest geschrieben Schranken - sollten zählen: Regeln zur Verantwortlichkeit, Zertifizierung und Zweckbindung, Abrufverfahren, Erforderlichkeit, Transparenz, Erhebung beim Betroffenen.
- Auch im juristischen Teil des Gutachtens sollte mehr zur **Datensparsamkeit** und ihrer Ableitung aus dem Erforderlichkeitsprinzip gesagt werden. Hier sollte unterschieden werden: die Datensparsamkeit auf der Ebene der Verfahrensgestaltung und die Erforderlichkeit bezogen auf einen bestimmten Zweck.

- Unzureichende Datensparsamkeit sollte als Unzulässigkeitskriterium ausgestaltet werden.
- Datensparsamkeit ist Auditierungsgesichtspunkt, nicht nur Kriterium für die Zulässigkeit oder Zielkriterium für die Verfahrensgestaltung.
- **Pseudonymität und Anonymität** sind nicht allein Fragen der Technik, sondern gehören auch in den rechtlichen Bereich. Dies sollte im Gutachten berücksichtigt werden. Dabei sollte beachtet werden, dass Pseudonymität und Anonymität weniger Schutzziele als vielmehr Mechanismen für einen wirksamen Datenschutz sind.
- **Transparenz** hat ihre Grenzen, daher sollten nicht übertriebene Hoffnung geweckt werden.
- Die **DV beim Betroffenen** als Maßnahme des Datenschutzes hat nur begrenzte Chancen, da ein zwangsweiser Selbstschutz kaum durchsetzbar sein wird. Generell eine Speicherung personenbezogener Daten beim Betroffenen selbst vorzusehen, ist illusorisch.
- Die Rolle der **betrieblichen/behördlichen Datenschutzbeauftragten** (bDSB) muss gestärkt werden.

Technik

- Datenschutz ist auch für die Technik ein **Akzeptanzfaktor**. Technik, die (aus Datenschutzgründen) nicht akzeptiert wird, ist unverkäuflich.
- Ein Verweis im Gesetz, der hinsichtlich des gesetzlich geforderten technischen Standards lediglich auf Fachliteratur verweist, ist nicht praktikabel, da es an der notwendigen Normierung fehlt.
- Technisch ist vieles **möglich, wenn** es sein muss – also **gesetzlich vorgeschrieben** ist.
- Für den **Selbstdatenschutz** muss es technische Systeme geben, die leicht zu handhaben sind – dies muss geregelt werden, möglicherweise als gesetzliche Verpflichtung.
- § 3a BDSG 2001 (Datenvermeidung und Datensparsamkeit) und § 9 BDSG (technische und organisatorische Maßnahmen) sollten zusammengeführt und einheitlich gestaltet werden.
- Technische Maßnahmen des Datenschutzes sollen im Gesetz überall dort **normiert** werden, wo sie notwendig sind. Daneben ist aber auch an eine Vorschrift ähnlich § 10 LDSG-NRW zu denken.
- **Datenvermeidungssysteme** könnten in den technischen und organisatorischen Ablauf eingebaut werden.
- Pflicht zur Löschung und Datenvermeidung muss bei der technischen Realisierung von DV-Systemen berücksichtigt werden.
- Wie werden die Interessen der **Bedarfsträger** an der Identität der Nutzer im Rahmen der Strafverfolgung berücksichtigt?
- Bei Bedarfsträgern besteht offensichtlich der Wunsch, Straftäter nur vom Schreibtisch aus verfolgen zu können. Man muss aber an die Kriminellen selbst ran.
- Möglichkeiten, Daten für die Strafverfolgung zu nutzen, wären black-box-systeme mit richterlicher Genehmigung zur Öffnung im konkreten Fall oder quick-freeze-Verfahren.
- **Datenspeicherung beim Betroffenen** selbst ist zu begrüßen. Probleme entstehen allerdings beim Management der Daten – siehe Chipkarten. Wie umfänglich soll dies protokolliert werden?
- Aktivitäten von anderen auf Datenverarbeitungsgeräten der Nutzer müssen immer angezeigt werden (Transparenz) – als Gebot zu formulieren!
- Der Selbstdatenschutz spielt bei der Verwendung von **Chipkarten** eine wichtige Rolle. Doch muss beachtet werden, dass die Nutzung von Daten keine Frage der Eigentumsordnung, sondern der Informationsordnung ist, in der der Betroffene aber auch der Datenver-

arbeiter Rechte an der Verwendung von Daten hat. Die Daten, die ein Arzt über einen Patienten erhebt, sind nicht das Eigentum des Patienten, sondern zugleich auch Daten über die Tätigkeit des Arztes, an denen er auch Nutzungsrechte haben muss. Diese sind mit den Rechten des Betroffenen in Einklang zu bringen.

- Bei einem „**Schubladensystem**“ auf Chipkarten entstehen Probleme, wenn dem Betroffenen das Recht gegeben wird, alle Daten preiszugeben, bspw. durch PIN für alle gespeicherten Daten.

Verbot mit Erlaubnisvorbehalt

- *Klarstellung der Gutachter:* Das Verbot mit Erlaubnisvorbehalt wird dem Grunde nach nicht aufgehoben, sondern durch die Grundsätze der Datenverarbeitung neu gestaltet.
- Das **„berechtigte“ Interesse** soll nicht mehr Rechtmäßigkeitsmaßstab sein, vielmehr ein „rechtliches“ Interesse oder dessen spezifische Ausformulierung. Dazu sollte das Gutachten – angesichts der politischen Brisanz (Interessen der Wirtschaft) – weitergehende Ausführungen enthalten.
- Die Gefahrenabwehr (auch im privatrechtlichen Sinne, z.B. Verfolgung von Rechtsansprüchen, Selbsthilfe) in den Vordergrund gerückt werden. Eine **Kategorie „private Gefahrenabwehr“** könnte z.B. den Schutz wichtiger Rechtsgüter umfassen.
- Es ist fraglich, ob man so weit gehen muss: Es gibt auch Daten, deren Verarbeitung durchaus durch ein berechtigtes Interesse gerechtfertigt wäre. Bsp.: Nutzung von Spenderadressen für die Werbung des DRK für die Blutspende.
- Vertragsabwicklung und Einwilligung/Zustimmung sind nicht identisch. Daher muss die **Zweckbestimmung** und die **Erforderlichkeit** der DV auch in Zukunft beibehalten werden. Verträge sollten eine Formulierung enthalten, dass DV zum Zwecke der Vertragserfüllung geschieht.
- Eine **Zweckänderung** sollte im Regelfall beim Betroffenen durch Nachfrage und Zustimmung abgesichert werden.
- Die **Erforderlichkeit** muss sich am praktischen täglichen Bedarf der DV ausrichten.

Datenverarbeitung mit gezieltem und mit ungezieltem Personenbezug

Klarstellung der Gutachter:

  - Die Unterscheidung ist zum einen notwendig, da es Ziel der Modernisierung des Datenschutzrechts ist, das TK-Recht zu integrieren.
  - Zum anderen fällt die bisherige Regelung in § 1 Abs. 3 BDSG zu temporären Dateien mit dem BDSG 2001 weg. Allerdings werden andere Rechtsfolgen vorgeschlagen als in dem bisherigen § 1 Abs. 3 BDSG.
  - Data Warehouse und Videoüberwachung sind als Beispiele herausgenommen worden, da sie ein eigenes Risikopotential enthalten und risikoadäquate Regelungen verlangen.
  - Ziel ist es, zu vermeiden, dass Datenschutzvorschriften sich der Intention des Datenschutzes entgegen stellen, indem zur Durchsetzung von bspw. Auskunftsansprüchen zusätzliche Daten gespeichert werden müssten.

- Für die Einführung unterschiedlicher Kategorien der DV könnte es notwendig sein, die **DSRL** zu ändern.
- Es sollte auf Generalklauseln (beispielhaften) im Gesetz verzichtet werden und statt dessen ein präziser Katalog möglichst spezifischer Fallgestaltungen erstellt werden.
- Wenn Datenverarbeitungskategorien mit unterschiedlichen Zulässigkeitsvoraussetzungen vorgesehen werden sollen, muss eine Verschlechterung gegenüber den bisherigen Regelungen des TK-Rechts, TDDSG verhindert werden.

Zustimmung

- Der **Begriff „Zustimmung“** entspricht dem Sprachgebrauch vieler Vorschläge. Er sollte in jedem Fall nur die vorherige Zustimmung umfassen. Gewollt ist die informierte vorherige Zustimmung zur DV.
- Ist es richtig, die **Zustimmung** zum zentralen Anker des Datenschutzes zu machen? Dies setzt Information und Verständnis voraus! Es besteht **Skepsis** hinsichtlich der Vorstellung vom **informierten Verbraucher**, da in der Regel keiner die Einwilligungsklausel wirklich studiert. Darüber hinaus sind vorgegebene Einwilligungsklauseln der Regelfall. Ebenso bestehen häufig „Zwangslagen“, die bei der Frage der Zulässigkeit der Zustimmung berücksichtigt werden müssen. Datenschutzrecht muss sich an Normalnutzer und nicht an Spezialisten orientieren – der Aufwand für einen effektiven Selbstdatenschutz muss gering sein. Ein angemessenes Schutzniveau muss auch ohne Zustimmung des Betroffenen bestehen.
- Erfahrungen mit der Einwilligung waren in der Vergangenheit dennoch gut, wenngleich die Anforderungen unterschiedlich hoch sind. Sie ist der **Schlüssel für die Betroffen**, an der DV beteiligt zu sein. Die Aufforderung zur aktiven Einwilligung wird das Interesse der Betroffenen wecken.
- Die **Grenzen der Einwilligung** müssen in den entsprechenden Paragrafen eingebaut werden. Es sind exakte Rahmenbedingungen notwendig, einzelne Fallbereiche sollten untersucht werden. Das BVerfG hat in seiner „Schuldenturmentscheidung“ Grenzen der Einwilligung gefordert, mithin auch Grenzen der DV. Daher sind solche auch erforderlich.
- Die Gewährleistungspflicht hat allerdings auch ihre Grenzen. Es gibt beispielsweise das „Recht sich zu verschulden“.
- Mit ausufernden Einwilligungen werden Tor und Tür für die Kommerzialisierung personenbezogener Daten geöffnet.
- *Replik:* Kommerzialisierung findet ohnehin statt. Dann sollte sie aber nicht an den Betroffenen vorbei geschehen. Die Kommerzialisierung der Daten wäre dann kein Problem, wenn diese ausdrücklich vereinbart ist. Ein Verbot würde auf Unverständnis der Bevölkerung stoßen, da sie durchaus auch bewusst und gewollt stattfindet. Man sollte sich vielmehr auf die umfassende Aufklärung und Unterrichtung konzentrieren.
- **Vorformulierte Einwilligungserklärungen** sind akzeptabel, wenn die unterschiedlichen Einwilligungstatbestände jeweils zustimmungsfähig sind, wenn ein Kopplungsverbot besteht und wenn bei Diensten der Grundversorgung auch immer eine datensparsame Variante angeboten wird (z.B. schufaloses Konto). Die Einwilligung muss fallbezogen erfolgen.
- Bei vorformulierten Erklärungen muss allerdings die Selbstregulierung eingreifen, Zertifizierungen als Verbandsregeln vorgesehen werden – Orientierung am AGBG. Verbraucherverbände müssen bei § 38 a BDSG 2001 berücksichtigt werden.
- Es gibt Vorschläge im Rahmen der Selbstregulierung datenschutzrechtliche „Universaldienste“ zu entwickeln. Zu klären ist deren Genehmigung. Ansätze finden sich in § 38 a BDSG 2001.
- Ein **Widerrufsrecht** sollte explizit vorgesehen werden.
- Es muss eine **Dokumentationspflicht** der Zustimmung geben.
- Sonderregeln könnten für pseudonymisierte Verfahren gelten mit einer opt-out Möglichkeit.
- Der angemessene Schutz muss durch ein gesetzlich festgeschriebenes Mindestmaß an Schutzmaßnahmen für den Betroffenen durch Verarbeitungsregeln erreicht werden und durch die Einwilligungsmöglichkeit des Betroffenen.

Selbstregulierung

- **Verbraucher** und **Kontrollstellen** sollen in die Selbstregulierung einbezogen werden.
- Der Verbraucher muss sicher sein, dass ihm ein Mindestmaß an Schutz gewährt wird (Internetregulierung).
- Wegen der Branchenbezogenheit der Selbstregulierung bedarf es der Abstimmung mit dem **Düsseldorfer Kreis**.
- **Gesetzliche Anerkennung** könnte Maßnahmen der Selbstregulierung für verbindlich erklärt werden. Wären Allgemeinverbindlichkeitserklärungen mit Sanktionen sinnvoll?
- Es wäre sinnvoll dafür eine **Bundesinstanz** zu installieren, da die Kontrolle durch die Aufsichtsbehörden schwierig wäre. Diese müsste eine Oberaufichts-Funktion haben. Die Instanz, die die Regulierung vornimmt, sollte selbständig kontrollieren können. Eine bundeseinheitliche Kontrollstellen ist notwendig, da unterschiedliche Standards verschiedener Stellen auf die Standortpolitik von Konzernen Einfluss haben könnten.
- Probleme bei der Installation einer Behörde könnten sich aus den Bund-Länder-Kompetenzen (Art. 87 Abs. 3 GG) ergeben, da der Bund kein Landeskoordinierungsgremium schaffen kann. Eine Möglichkeit könnte ein Staatsvertrag sein. Schlägt vor, dass Berlin für ein solches Gremium zuständig sein sollte, dann andere Länder beteiligt.
- Der Bund kann die Zuständigkeit regeln. Dabei können auch die Länder mit Zuständigkeiten bedacht werden.
- Die Konferenz könnte die Länder auffordern, einen entsprechenden **Staatsvertrag** zu schließen?
- Es wird vor einer frühzeitigen Festlegung gewarnt. Zurückhaltung in dieser Beziehung könnte angebracht sein, da zur Zeit Verbände zuständig sind (Berlin, Hamburg, NRW).
- Es sollte eine klare Aussage getroffen werden, dass eine bundesweite Zuständigkeit angesichts der föderalen Struktur der Bundesrepublik abgelehnt wird.
- Die Beteiligung der Kontrollstellen wäre kontraproduktiv zum Unabhängigkeitsstreben der Aufsichtsbehörden. Landesbehörden sollten jeweils zuständig sein.
- Bspw. schreiten die **Aufsichtsbehörden** bei Umweltaudits solange nicht ein, wie eine Auditierung vorliegt. Sie erfüllen eine Auffangfunktion für das staatliche Kontrollnetz.
- Die **Auditierung** ist ein betriebsbezogenes Verfahren. Sie ist ein Plus gegenüber den gesetzlichen Anforderungen des Datenschutzrechts. Etwas anderes ist die Selbstbeschränkung durch Verbände – Bsp.: Regelungen der Presse.

Kontrollstellen

- Die **Rechtsaufsicht** ist praktisch bedeutungslos.
- *Replik:* Die Rechtsaufsicht nähert sich faktisch der Fachaufsicht, wenn Gesetze sehr detailliert sind. Daher sollte die Rechtsaufsicht verschwinden. Die Effektivität der politischen Kontrolle ist bei den Datenschutzbeauftragten stärker als bei Regierungen.
- Es bestehen Zweifel daran, dass man die derzeitige Konstruktion des BfD – Rechtsaufsicht der BReg – ändern kann.
- Je vielfältiger die Einwirkungsmöglichkeiten der Kontrollstellen sind, um so wichtiger ist die Aufsicht. Daher wird vorgeschlagen, die Datenschutzbeauftragten in die Verfassung aufzunehmen, wenngleich deren Unabhängigkeit in gewissem Widerspruch zum Demokratieprinzip steht.
- Eine **Abwahlmöglichkeit** des Datenschutzbeauftragten birgt Gefahren für die Unabhängigkeit der Datenschutzbeauftragten! Es bestünde die Gefahr des „Rosinenpickens“.

- Andererseits würde eine Abwahlmöglichkeit die Legitimationsdebatte erleichtern. Sie könnte eine notwendige Kompensation für die Aufhebung von Rechts- und Dienstaufsicht sein.
- Wären **kürzere Amtszeiten** eine Alternative?
- Gefahren größerer **Einwirkungsbefugnisse** sollten nicht außer Acht gelassen werden:
- · Begehrlichkeiten auf Einflussnahme werden zunehmen,
- · gerichtliche Überprüfung schwächt die Position der Datenschutzbeauftragten.
- Die **„forensische Verstrickung“** ist ein wichtiges Mittel. Bisher haben die Datenschutzbeauftragten im luftleeren Raum agiert.
- Eine **Bußgeldbehörde**, die Verwaltungszwang anwenden kann, sollte auch die Funktion einer Verwaltungsbehörde haben.
- Man sollte politisch-taktisch denken. Eine größere Nähe zum Parlament ist anzustreben. Dadurch kann die Legitimation der Datenschutzbeauftragten gestärkt werden.
- Weitere Befugnisse sind im privaten Bereich unproblematisch. Schwieriger ist es im öffentlichen Bereich, „effektive Maßnahmen“ vorzusehen. Eine Feststellungsklage und ein generelles Klagerecht sollten ermöglicht werden.
- Die Einbeziehung der LfD/Aufsichtsbehörden in die Vorabkontrolle ist nicht zu bewältigen. Daher sollte sie nicht vorgesehen werden.

Einbeziehung juristischer Personen

- Es bestehen Zweifel an der Notwendigkeit, juristische Personen unter den Schutz des Datenschutzrechts zu stellen.
- Diesbezüglich sprechen die **Neue-Heimat-Entscheidung** und das **Flick-Urteil** aber eine eindeutige Sprache. Gleichwohl ist die Frage sehr problematisch.
- Mit einer Einbeziehung juristischer Personen könnte die **grundrechtliche Verankerung** des Datenschutze im informationellen Selbstbestimmungsrecht aufgegeben werden.
- Praktische Beispiele zeigen, warum eine unterschiedliche Behandlung sinnvoll ist, bspw. Rundfunkstaatsvertrag.
- Statt einer abstrakten Darstellung des Problem, sollte das Gutachten **Beispiele** für die Notwendigkeit einer Einbeziehung juristischer Personen aufführen.

---

5. Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

- 2. Stufe der Novellierung des Bundesdatenschutzgesetzes -

Die Datenschutzbeauftragten des Bundes und der Länder haben sich am 03. und 04.04.2001 intensiv mit dem vom Gutachterausschuss vorgelegten Gutachtendesign vom 14.12.2000 (in der Fassung vom 26.03.2001) für eine 2. Stufe der Novellierung des Bundesdatenschutzgesetzes befasst. Sie unterstützen nachhaltig das Anliegen, den Datenschutz grundlegend zu modernisieren. Die Ausführungen im ersten Teil des Gutachtendesigns zur Notwendigkeit der Novellierung des Datenschutzrechts beschreiben die Ausgangssituation im Wesentlichen zutreffend.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihren Entschließungen vom 23./24.10.1997, 5./6.10.1998, 25./26.3.1999 und 12./13.10.2000 wesentliche Aufgabenfelder für eine Modernisierung des Datenschutzrechts benannt. Diese werden im Gutachtendesign aufgegriffen. So etwa die Forderungen der Konferenz,

- den Grundrechtscharakter des Rechts auf informationelle Selbstbestimmung klar herauszustellen
- ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und nicht-öffentlichen Bereich, soweit die verfassungsrechtlich verankerten Strukturunterschiede dies zulassen, verbunden mit einheitlichen Kontrollstellen für beide Bereiche
- nach klarer und einfacher Gesetzessprache.

  Darüber hinaus wird es eine wichtige Aufgabe im Rahmen der Novellierung sein, geeignete Maßnahmen gegen das Erstellen von Persönlichkeitsprofilen zu entwickeln.

Die Lösungsansätze des vorliegenden Designs werden im Wesentlichen unterstützt. Dabei weist die Konferenz zusätzlich auf Folgendes hin:

- Die im Gutachtendesign vorgeschlagene Struktur eines allgemeinen Datenschutzgesetzes, das allgemein verbindliche Regeln für alle Bereiche enthält und bereichsspezifische Regelungen auf ein notwendiges Maß zurückdrängt ist grundsätzlich richtig. Es sind allerdings die Bereiche festzulegen, die aufgrund des besonderen Gefährdungspotentials eigener Regelungen bedürfen.

  Zudem sollten die Verarbeitungsgrundsätze, die auf S. 10 ff des Gutachtendesigns beschrieben sind, gestärkt und klar herausgearbeitet werden.

- Eine zentrale Norm, die die Grundsätze des technischen Datenschutzes festlegt, ist sinnvoll. Sie sollte aber durch Detailregelungen ergänzt werden, die darauf abzielen, die materiellen Datenschutzregelungen durch technische Maßnahmen zu unterstützen.

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken.

- Der bisherige Grundsatz, dass Datenverarbeitung nur dann möglich ist, wenn es eine Erlaubnisnorm dafür gibt oder im Einzelfall eine Einwilligung der betroffenen Person vorliegt, muss beibehalten werden. Nur dies entspricht den verfassungs- und europarechtlichen Vorgaben. Dabei ist es im Interesse des Selbstbestimmungsrechts der Betroffenen, wenn das Instrument der Einwilligung grundsätzlich gestärkt wird. Welche Grenzen dabei im Interesse des Allgemeinwohls zu ziehen sind, ist noch präzise festzulegen. Es wird in diesem Zusammenhang jedenfalls zu bedenken sein, ob bei einer Stärkung der Einwilligung einerseits, andererseits das Tatbestandsmerkmal - berechtigtes Interesse - als Voraussetzung für eine Datenverarbeitung, die ohne Einwilligung erfolgt, zu schwach ist.
- Es ist zu begrüßen, dass die Videoüberwachung und das Datamining nicht mehr als Beispiele für eine Datenerhebung ohne gezielten Personenbezug gelten, sondern jeweils Gegenstand eigener Regelungen sein sollen. Wenn auch mit den Begriffen der Datenerhebung mit „gezieltem/ nicht gezieltem Personenbezug“ tatsächlich vorhandene Lebenssachverhalte beschrieben werden sollen, so hat doch die Diskussion gezeigt, dass die Zuordnung zu solchen Begriffen stark durch die subjektive Intention derjenigen bestimmt wird, die Daten erheben. Als gesetzliche Tatbestandsmerkmale sind die Begriffe daher ungeeignet. Das Gutachten wird für die jeweiligen Lebenssachverhalte Lösungen anbieten müssen. Es sollte jedoch wegen der mit der bisherigen Terminologie verbundenen Abgrenzungsschwierigkeiten solche unbestimmten und von subjektiven Elementen beeinflussten Begriffe vermeiden. Es sollte auch deshalb auf diese Begriffe verzichtet werden, weil sie sich in der EG-Datenschutzrichtlinie nicht wiederfinden und einem einheitlichen Datenschutzrecht auf europäischer Ebene nicht zuträglich sind. Eine Lösung könnte ein nach objektiven Kriterien festgelegter Katalog von Fallgruppen sein, der die in Betracht gezogenen Sachverhalte beschreibt. Dabei wird die Schwierigkeit für die Gutachter darin bestehen, herauszuarbeiten, wann eine - mit den bisherigen Begriffen ausgedrückt - Datenerhebung ohne gezielten Personenbezug in eine mit gezieltem Personenbezug umschlägt.
- Die dem Gutachtendesign zugrunde liegenden Überlegungen einer eigenen datenschutzrechtlichen Kategorie der Einwilligung sind sinnvoll. Durch den gewählten Begriff „Zustimmung“ wird jedoch ein wesentliches Element der datenschutzrechtlichen Einwilligung, nämlich die Tatsache, dass sie schon vor der Datenerhebung abgegeben werden muss, verdeckt. Es sollte bei dem Begriff Einwilligung bleiben, da hier, in der Rechtssprache allgemein anerkannt, eine im Voraus abzugebende Erklärung gemeint ist.

  Soll die Einwilligung als Ausdruck der informationellen Selbstbestimmung gestärkt werden, sind zugleich ihre Konturen zu schärfen. Vor allem die Freiwilligkeit der Einwilligung muss sichergestellt werden. Es wird Lösungen geben müssen, Die für soziale und faktische Zwangslagen Vorsorge treffen. Es muss vermieden werden, dass Einwilligungen letztlich unwillentlich, aber unter sozialem Druck doch abgegeben werden. Außerdem sind dort Vorkehrungen nötig, wo eine Mehrheit der Betroffenen in den Datenverarbeitungsprozess einwilligt und die Verweigerung der Einwilligung zu eine Außenseiterstellung führt. Auch bei Gewährung finanzieller Anreize für die Einwilligung sind Sicherheitskriterien oder Koppelungsverbote notwendig.

  Dort, wo Einwilligungen in Datenverarbeitung im Zusammenhang mit Massengeschäften gerade auch der technischen und infrastrukturellen Grundversorgung abgegeben werden sollen, sind Lösungen über eine Selbstregulierung vorzuse-

hen. Es können ggf. Texte für Formulareinwilligungen von den jeweiligen Unternehmensbranchen unter breiter Beteiligung von Verbänden ausgehandelt und der Aufsichtsbehörde zur Genehmigung vorgelegt werden.

- In Bezug auf Selbstregulierungsmechanismen sind einerseits Auditierungsverfahren zu betrachten. Andererseits - und klar von Auditierungsverfahren zu trennen - sind Instrumente der Selbstregulierung auf Betriebs- oder Verbandsebene denkbar.

  Für die Auditierung ist gesetzlich sicherzustellen, dass sie ausschließlich durch zertifizierte Gutachter durchgeführt wird und dass nur solche Verfahren auditiert werden, die über den gesetzlich geregelten Mindeststandard des Datenschutzes hinausgehen.

  Verhaltensregeln, die im Rahmen betrieblicher Selbstregulierung bzw. Selbstregulierung durch Verbände eingeführt werden sollen, müssen sich an die gesetzlichen Vorgaben halten und können diese nicht unterlaufen. Der gesetzliche Rahmen für solche Verhaltensregeln muss festlegen, wie eine Allgemeinverbindlichkeit der Regeln erreicht wird. Er muss darüber hinaus wirksame Sanktionsmechanismen vorsehen, für den Fall, dass gegen solche Verhaltensregeln verstoßen wird. Sinnvoll erscheint ein gestuftes Sanktionssystem, bei dem in der ersten Stufe Sanktionen durch den Verband und erst in der zweiten Stufe bei besonders gravierenden oder wiederholten Verstößen Sanktionen durch die Kontrollstelle(n) verhängt werden.

  Die betrieblichen Datenschutzbeauftragten müssen in die Aufstellung und Kontrolle von Verhaltensregeln einbezogen werden. Ihre Position soll auf diese Weise gestärkt werden. Darüber hinaus muss es eine breite Beteiligung von Verbänden geben, die die Interessen derjenigen vertreten, die durch bestimmte Verhaltensregeln betroffen sind. Es sollte über ein Klagerecht von Verbänden gegen Verhaltensregeln nachgedacht werden.

  Insgesamt ist ein koordiniertes Vorgehen der Länder in Fragen der Selbstregulierung anzustreben. Vor allem über eine möglicherweise erforderliche Vereinbarung über Zuständigkeiten von Kontrollstellen sollte Einigung erzielt werden.

  Die nach der EG-Richtlinie notwendige Unabhängigkeit der Kontrollstellen gebietet es, sie von jeder Aufsicht in der Sache freizustellen. Maßnahmen der persönlichen Dienstaufsicht gegen Datenschutzbeauftragte sind nach den gleichen Kriterien zulässig wie bei Richterinnen und Richtern.

  Bedenken bestehen gegen das Einbinden der Kontrollstellen in die Vorabkontrolle, die durch die betrieblichen Datenschutzbeauftragten vorzunehmen ist. Dadurch würde die Stellung der betrieblichen Datenschutzbeauftragten geschwächt. Dies würde den erklärten Grundsätzen des Gutachtendesigns nicht entsprechen.

Die bisherige Arbeit des Gutachterausschusses und die fruchtbare Diskussion mit den Gutachtern hat gezeigt, dass die dargestellten Reformansätze zukunftsweisend sind. Die Konferenz setzt sich entschieden für eine zweite Stufe der Novellierung des Bundesdatenschutzgesetzes ein. Sie legt dabei besonderen Wert darauf, dass die Innovation in der Weise erfolgt, dass das bisherige hohe Niveau des deutschen Datenschutzrechts beibehalten und ausgebaut wird.

6. Stellungnahme des Bundesverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. (Auszug)

Forderungen des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. zur 2. Phase der Novellierung des Bundesdatenschutzgesetzes (BDSG)

*BvD-Arbeitskreis "Die zukünftige Entwicklung des BDSG in Deutschland" *)*

Zusammenfassung

Der Arbeitskreis "Die zukünftige Entwicklung des BDSG in Deutschland" des BvD hat sich nach der Bundestagswahl im Frühjahr 1999 gebildet, um die gesetzgeberische Arbeit zur Novellierung des BDSG zu begleiten.

Der Arbeitskreis (AK) legt hiermit seine ersten Arbeitsergebnisse vor. Schwerpunkte sind folgende:

- *technikorientierte Begriffsbestimmungen (Ziffer 1),*
- *neue Überlegungen zur Qualifikation und Tätigkeit des DSB (Ziffer 2),*
- *Neuregelung der Zusammenarbeit zwischen DSB und Betriebsrat (Ziffer 2.2),*
- *Ersatz des § 9 und Anlage durch die Schutzziele der IT-Sicherheit (Ziffer 3),*
- *Zusammenfassen von bereichsspezifischen Regelungen (Ziffer 4),*
- *Überlegungen zu einem Arbeitnehmer-Datenschutzgesetz (Ziffer 4.1),*
- *Verfassungsrang des Datenschutzes (Ziffer 7).*

Das vorliegende Manuskript ist die Kurzfassung eines Arbeitspapiers, das der Arbeitskreis "Die zukünftige Entwicklung des BDSG in Deutschland" des BvD erstellt hat. Dieses Papier kann über die Kontaktadresse des Arbeitskreises (s. S. 7) bezogen werden.

1 Begriffe im Datenschutzrecht

1.1 Bürgernahe Sprache

Wie kaum ein anderes Gesetz wird das BDSG in der praktischen Arbeit von Nichtjuristen angewandt. Auf der anderen Seite enthält gerade das BDSG eine Vielzahl unbestimmter Rechtsbegriffe. Dies gilt leider auch für den BDSG-E.

Deshalb fordert der BvD, dass das BDSG in seinem Wortlaut bürgernah, verständlich und eindeutig (normenklar) sein muss.

Der AK des BvD hat sich mit den Begriffen des Datenschutzes intensiv beschäftigt. Er will im vorliegenden Arbeitspapier besonders das Augenmerk auf den Begriff der **Erhebung** richten.

Er fordert daher die Aufnahme des Begriffs der Erhebung in den § 3 Abs. 4 **als erste Stufe der Verarbeitung**, wie es die EU-Richtlinie im Art. 2 b vorschreibt und wie es auch dem Verständnis der Informatik entspricht.

1.2 Begriffe, die sich an der IT-Sicherheit orientieren

Der AK hat sich grundlegende Überlegungen zu den technischen und orga-nisatorischen Maßnahmen des Datenschutzes gemacht. Auch hier muss eine einheitliche Sprache von Datenschützern und Informatikern hergestellt werden. Dies erfordert u.a. auch die Einführung

der **Begriffe Verfügbarkeit, Vertraulichkeit, Integrität** und **Zurechenbarkeit** in den Gesetzestext. Näheres ist unter Ziffer 3 ausgeführt.

2 Der Beauftragte für den Datenschutz (DSB)

Der Datenschutzbeauftragte ist fachlich und disziplinarisch direkt der Leitung des Unternehmens bzw. der Behörde zu unterstellen.

Zu seinen **grundlegenden Qualifikationen** gehören

- Fachkompetenz
- Methodenkompetenz
- Sozialkompetenz
- Führungskompetenz
- Unternehmerische Kompetenz.

(siehe dazu Anhang 2 auf S. 8 und Anhang 3 auf S. 9).).

Neben den grundlegenden Qualifikationen sind der Aufsichtsbehörde das ihm zur Verfügung stehende Zeitbudget, das Fehlen von Interessenskonflikten in Verbindung mit sonstigen Tätigkeiten, sowie die organisatorische Einbindung in das Unternehmen nachzuweisen.

2.1 Stellung im Unternehmen

Die Vorschriften sollen in gleicher Weise für den behördlichen wie auch für den betrieblichen Datenschutzbeauftragten gelten.

Es ist anzustreben, dass ein DSB grundsätzlich keine zusätzlichen Aufgaben erfüllen soll. Dies soll auch grundsätzlich für den externen DSB Geltung ha-ben. Für den Prüfungskatalog der Aufsichtsbehörde soll dies ein zu kontrol-lierendes Kriterium sein.

Für den DSB ist eine Übernahme der “Betriebsräteregelung” für erweiterten Kündigungsschutz zu erwirken.

2.2 Verhältnis des DSB zum Betriebsrat/Personalrat

Notwendig ist eine Regelung über die Zusammenarbeit beider Stellen im Sinne einer gemeinsamen Zielsetzung zum Schutz von Mitarbeiterdaten und zur Wahrung der Rechte der Betroffenen.

Der BvD fordert unabhängig davon ein Kontrollrecht des DSB auch im Bereich des Betriebsrates / Personalrates, da dieser Teil der verantwortlichen Stelle ist. Dazu muss aber im Gesetz festgeschrieben werden, dass Beanstandungen im Betriebsrats- / Personalratsbereich nicht der Geschäftsleitung, sondern dem Betriebsrats- / Personalratsvorsitzenden gegenüber ausgesprochen werden.

Ein Vorschlag des BvD zur Neuformulierung des § 4f findet sich im Anhang 2 auf S. 8.

3 Maßnahmen der IT-Sicherheit

Es gilt zu verhindern, dass aufgrund technischer Weiterentwicklungen ein daraus resultierender ständiger Gesetzesänderungsbedarf entsteht.

Das Gesetz muss auch die Sprache der Technik sprechen, damit die “Tech-niker”, die es anwenden sollen, sich darin wiederfinden und es verstehen. Es soll deshalb, wie schon gesagt, eine einheitliche Sprache von Datenschützern und Informatikern hergestellt werden. Dazu muss die Anlage zu § 9 durch die Schutzziele der IT-Sicherheit Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit ersetzt werden.

Diese Schutzziele werden im Datenschutz begrenzt durch die Prinzipien der Erforderlichkeit, Datenvermeidung und Datensparsamkeit.

3.1 Vertraulichkeit

Die **Vertraulichkeit** bedeutet Zugriff auf personenbezogene Daten und In-formationen über Kommunikationsbeziehungen so zu gestalten, dass sie ausschließlich zur rechtmäßigen Aufgabenerfüllung im Rahmen der Zustän-digkeit verwendet werden.

Vertraulichkeit bezieht sich sowohl auf Daten als auch auf Verbindungsdaten und die Kommunikation selbst.

3.2 Verfügbarkeit

Die **Verfügbarkeit** von Inhalten und Kommunikationswegen bedeutet Si-cherheit gegen Verlust oder Beeinträchtigung der Funktionsfähigkeit von Systemen. In der heutigen Kommunikationsgesellschaft hängt das Persön-lichkeitsrecht des Menschen auch von der Funktionalität von Rechnern und Netzen ab.

3.3 Integrität

Die **Integrität** von Inhalten zielt auf die Richtigkeit und Vollständigkeit von personenbezogenen Daten innerhalb des jeweiligen Sachzusammenhangs zum Schutz des Betroffenen. Dabei steht die Integrität zwingend unter dem Vorbehalt der Datensparsamkeit.

3.4 Zurechenbarkeit

Die **Zurechenbarkeit** von Inhalten und Kommunikationspartnern bedeutet sicherzustellen, dass jederzeit festgestellt werden kann, wer wann welche Daten in welcher Form verwendet hat (Revisionsfähigkeit). Diese Daten wer-den protokolliert. Um das Ziel der Datensparsamkeit nicht zu unterlaufen, dürfen Protokolldaten nur für Zwecke der Datenschutzkontrolle, der Datensi-cherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.

Eine Verwendung dieser Daten zu Leistungs- und Verhaltenskontrollen ist verboten. Man muss sicher sein, dass der Kommunikationspartner auch wirklich der ist, der er vorgibt zu sein.

4 Bereichsspezifische Regelungen

Um die Transparenz, Handhabung und Umsetzung des Datenschutzes zu erleichtern, muss der Gefahr einer Aushöhlung des BDSG durch bereichs-spezifische Regelungen begegnet werden. Deshalb ist ein großer Teil grund-sätzlicher Datenschutzbestimmungen in einem allgemeinen Teil des Daten-schutzgesetzes zusammenzufassen.

Nur bereichsspezifische Tatbestände sind in besonderen Abschnitten des Gesetzes oder in speziellen Gesetzen (z. B. Arbeitnehmerdatenschutz) zu regeln.

Im Übrigen sind öffentliche und nicht-öffentliche Stellen den gleichen Datenschutzkriterien zu unterwerfen.

4.1 Schaffung eines Arbeitnehmerdatenschutzgesetzes

Die Arbeitswelt wird zunehmend durch die modernen Formen der Informations- und Kommunikationstechniken geprägt. Von der Wirtschaft und Verwaltung werden zur Zeit Fakten geschaffen, die im nachhinein durch den Gesetzgeber nicht mehr ohne weiteres zu beeinflussen sind.

Daher fordert der BvD die Schaffung eines Arbeitnehmerdatenschutz-gesetzes, wie es von zahlreichen anderen Gruppierungen seit langem verlangt wird.

5 Stellung des Bundesbeauftragten für den Datenschutz

Der BvD fordert Anbindung des Bundesbeauftragten für den Datenschutz direkt beim Bundestag mit dem Ziel der Unabhängigkeit und Bürgernähe.

6 Betroffenenrechte

Der BvD fordert Aufnahme des Rechtes auf Auskunft über den Verwen-dungszweck von Daten in die Betroffenenrechte.

7 Verfassungsrang des Datenschutzes

Der BvD fordert die Aufnahme des Datenschutzes als Grundrecht in die Verfassung.

Nachdem die Regierungschefs in Nizza die Aufnahme des Datenschutzes in die EU-Grundrechtscharta beschlossen haben, sowie dies bereits in der Mehrzahl der Länderverfassungen geschehen ist, sieht es der BvD nur als konsequent an, dies auch auf Bundesebene zu tun.

Ulm, den 23. Februar 2001

Anhang 2:

Formulierungsvorschlag des BvD zum § 4 f des BDSG-E

Der neue § 4 f soll gemäß Vorschlag des BvD wie folgt formuliert werden:

(1) Stellen, die personenbezogene Daten automatisiert verarbeiten und hier-bei in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben unter Beteiligung der Mitarbeitervertretung einen Beauftragten für den Da-tenschutz schriftlich zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer zur verantwortlichen Stelle entweder in einem Dienst- oder Arbeitsverhältnis steht (interner Datenschutzbeauftragter) oder wer mit der Stelle einen entsprechenden Vertrag mit einer Mindestlaufzeit von 5 Jahren abgeschlossen hat (externer Datenschutzbeauftragter).

(3) Der Beauftragte für den Datenschutz muss die erforderliche persönliche und fachliche Qualifikation und Eignung besitzen. Hierzu gehören insbesondere Fachkompetenz, Methodenkompetenz, Sozialkompetenz, Führungskompetenz, unternehmerische Kompetenz und das Fehlen von Interessenkonflikten. Zur Fachkompetenz gehören dem Stand der Technik entsprechende Kenntnisse in der Informationstechnik und die Fähigkeit, die Vorschriften dieses Gesetzes und der anderen den Umgang mit personenbezogenen Daten betreffenden Rechtsvorschriften anwenden zu können. Zum Erwerb und zur Pflege dieser Fähigkeiten und Kenntnisse hat die verantwortliche Stelle dem Datenschutzbeauftragten die gebotene Fortbildung zu ermöglichen und beim internen Datenschutzbeauftragten die entsprechenden Kosten zu übernehmen.

(4) Der Datenschutzbeauftragte ist dem Leiter oder dem Leitungsorgan der verantwortlichen Stelle unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Seine Bestellung darf nur widerrufen werden auf Verlangen der zuständigen Datenschutzkontrollinstanz oder in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches; dies gilt auch für seine Tätigkeit außerhalb der Datenschutzaufgaben.

(5) Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Dies gilt für den internen Datenschutzbeauftragten auch für die Ausübung von Tätigkeiten außerhalb seiner Freistellung als Datenschutzbeauftragter.

(6) Die verantwortliche Stelle hat den Beauftragten für den Datenschutz bei der Ausführung seiner Aufgaben zu unterstützen. Er ist über Vorhaben der Informationsverarbeitung rechtzeitig zu unterrichten. Er ist zur Wahrnehmung seiner Aufgaben freizustellen und angemessen mit personellen und sachlichen Mitteln auszustatten. Mitarbeiter sowie Mitarbeitervertretungen können sich jederzeit an den Datenschutzbeauftragten wenden. Der Datenschutzbeauftragte kann sich jederzeit an die zuständige Datenschutzkontrollinstanz wenden.

Impressum:

Herausgeber:
Bundesministerium des Innern
Referat Öffentlichkeitsarbeit
Alt-Moabit 101 D
10559 Berlin
September 2001

Gutachter:
Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka

Redaktion:
Referat V7

Druck:
Möller Druck, Berlin