Büro Vatter AG
Politikforschung & -beratung

Evaluation des Bundesgesetzes über den Datenschutz

Schlussbericht

Büro Vatter: Christian Bolliger, Marius Féraud

Institut für Europarecht, Universität Freiburg: Astrid Epiney, Julia Hänni

Bern, 10. März 2011

Zusammenfassung

Der vorliegende Bericht stellt die Ergebnisse der im Jahr 2010 im Auftrag des Bundesamts für Justiz durchgeführten Evaluation des Bundesgesetzes über den Datenschutz (DSG) dar. Das 1993 in Kraft getretene DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

►Gegenstand. Im Vordergrund der Evaluation standen die zwei zentralen Wirkungsmechanismen des DSG. Erstens wurde untersucht, inwieweit *datenschutzrechtliche Ansprüche auf dem Gerichtsweg durchgesetzt werden können.* Den zweiten Schwerpunkt bildete der *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)*: seine institutionelle Stellung und Unabhängigkeit, seine Organisation und seine Wirksamkeit wurden untersucht. Ein besonderes Augenmerk lag auf der Frage, wie die seit dem Inkrafttreten des DSG im Jahr 1993 zu beobachtende *Entwicklung der Informations- und Kommunikationstechnologien* die Wirksamkeit des Datenschutzgesetzes beeinflusst hat. Ebenso waren die *Bedürfnisse, Kompetenzen und Interessen der Betroffenen sowie der Datenbearbeiter* zu beleuchten.

►Vorgehen. Zur Beantwortung der vorgegebenen Forschungsfragen wurden 28 *halbstrukturierte Interviews* mit Rechts- und Technologieexperten, mit Interessenvertretern, mit Datenschutzverantwortlichen und mit Vertreterinnen und Vertretern des EDÖB geführt. Weiter wurden *statistische Materialen sowie Arbeitsdokumente und Veröffentlichungen des EDÖB* analysiert und ausgewertet. Verschiedene Aktivitätsbereiche des EDÖB wurden im Rahmen von *zehn Fallstudien* vertieft untersucht. Eine *Repräsentativumfrage* bei 1014 Personen hatte die datenschutzbezogenen Einstellungen, das Wissen und das Verhalten der Bevölkerung zum Gegenstand. Die *Rechtsprechung* zu den datenschutzrechtlichen Einsichts- und Durchsetzungsrechten Einzelner wurde anhand von 269 Urteilen kantonaler und nationaler gerichtlicher Instanzen analysiert. Eine weitere Grundlage dieser Evaluation war der vom Schweizerischen Institut für Rechtsvergleichung (SIR) erarbeitete Vergleich verschiedener *Aspekte des Datenschutzrechts in zehn Ländern*.

Umfeld des Datenschutzgesetzes: Technologie, Bearbeiter, Betroffene

►Technologische Entwicklung als Herausforderung. Die technologische Entwicklung seit dem Inkrafttreten des Gesetzes hat zu einer Vervielfachung der Möglichkeiten geführt, persönliche Daten zu erheben, miteinander zu verknüpfen, weiterzugeben und auszuwerten. Drei Entwicklungen sind in Bezug auf die Wirksamkeit des DSG besonders bedeutsam. Es ist erstens zu einer *Mengenausweitung an Datenbearbeitungen* gekommen, was insgesamt zu einem grösseren Missbrauchspotenzial führt. Zu den weiterhin vorkommenden Bearbeitungen, die gut identifizierbar sind, sind zweitens solche gekommen, die weder für die Betroffenen noch für den EDÖB ohne weiteres erkennbar sind; diese *intransparenten Bearbeitungen* erschweren den Selbstschutz der Betroffenen und die Kontrolle durch das Aufsichtsorgan. Insbesondere mit dem Internet treten drittens zunehmend private Datenbearbeiter auf, die vom Ausland her *grenzüberschreitend* agieren und sich so dem Zugriff der Betroffenen und des EDÖB weitgehend entziehen.

►Pragmatische Datenbearbeiter. Sowohl bei den öffentlichen als auch bei den privaten Datenbearbeitern gibt es Unterschiede hinsichtlich ihrer Sensibilität für den Datenschutz. Ein Grund

für den insgesamt eher *pragmatischen Umgang mit den Vorschriften des DSG* dürfte die *geringe Wahrscheinlichkeit einer Sanktion* sein. Insbesondere im Internet besteht zudem ein starker Anreiz, mit möglichst präzisen Persönlichkeitsprofilen zu handeln. Gleichzeitig ergaben sich deutliche Hinweise, wonach vor allem das Risiko eines *Imageschadens* (bei privaten Bearbeitern) oder eines *Vertrauensverlustes* (bei Bundesorganen), das Verhalten zugunsten des Datenschutzes zu beeinflussen vermag. Bei der Datenbearbeitung durch Bundesorgane wirken das Erfordernis einer gesetzlichen Grundlage und der damit verbundene transparente Entscheidungsprozess zusätzlich im Sinne des Datenschutzes.

►Bevölkerung will Schutz, ist aber teilweise nachlässig und überfordert. Laut der Bevölkerungsumfrage will die grosse Mehrheit der Bevölkerung an den neuen Möglichkeiten des Informationsaustauschs teilhaben. Gleichzeitig *empfindet sie den Schutz ihrer persönlichen Daten als wichtig* – unabhängig davon, ob es sich um klassische, übersichtliche oder um neue, unübersichtliche Konstellationen z.B. im Internet handelt. Dennoch schützen sich die Betroffenen *nicht immer konsequent* selbst, fühlen sich bisweilen *überfordert* oder *unterschätzen* die bestehenden Möglichkeiten der Datenbearbeitung und deren Risiken. Die bisweilen grosszügige Preisgabe persönlicher Daten dürfte auch damit zusammenhängen, dass das *Risiko eines Datenmissbrauchs und seiner Folgen als diffus und unwahrscheinlich wahrgenommen* wird, zumindest im Vergleich zum unmittelbaren Nutzen des jeweiligen Angebots.

Einklagbare Datenschutzrechte der Betroffenen

►Gesamtbilanz. Gemäss der Analyse der Rechtsprechung *kommt es selten vor, dass betroffene Personen den Rechtsweg* beschreiten, wobei es Unterschiede zwischen den verschiedenen Rechtsansprüchen gibt. *Anwendungen neuer Technologien sind praktisch nie Gegenstand* gerichtlicher Auseinandersetzungen.

►Recht auf Auskunft. Von den Einsichts- und Durchsetzungsrechten wird das Recht auf Auskunft gemäss Art. 8 DSG (bei Bearbeitungen von Bundesorganen) *am häufigsten* geltend gemacht. Dies gilt insbesondere für Sachverhaltskonstellationen, bei denen betroffene Personen durch ein vorgängiges Verfahren besonders auf die Datenbearbeitung sensibilisiert wurden.

►Durchsetzungsrechte gegenüber privaten Datenbearbeitern. Den Durchsetzungsrechten gegenüber privaten Datenbearbeitern (Art. 15 DSG) auf Berichtigung, Löschung, Sperrung und Vermerkung von Daten *kommt kaum eine eigenständige Bedeutung zu*. Diese Bestimmung erlangt nur zusammen mit Art. 28 ZGB eine gewisse, aber eben auch beschränkte Bedeutung.

►Durchsetzungsrechte gegenüber Bundesorganen. Datenbearbeitungen von Bundesorganen sind *Gegenstand einiger Urteile* der höheren Gerichte (Art. 25 DSG). Allerdings beziehen sich die meisten Begehren auf die Berichtigung (vermeintlich) unrichtiger Daten in einigen wenigen Sachbereichen. Soweit es um die Zulässigkeit einer Datenbearbeitung als solche geht, steht in der Regel die *Existenz einer ausreichenden gesetzlichen Grundlage* zur Debatte.

► Erklärungsansätze für die geringe Nutzung. Als mögliche Erklärungen für die geringe Nutzung der Durchsetzungsrechte können erstens die vermutlich *geringe Bekanntheit* der Durchsetzungsrechte und des Rechtswegs sowie das geringe Wissen über die Anwendung dieser Rechte

genannt werden. Zweitens dürfte aus Sicht der Betroffenen ein vergleichsweise *beträchtlicher Aufwand* einer Klage einem *diffusen und nicht gesicherten Nutzen* gegenüberstehen. Je nach Situation kann der Rechtsweg für die Betroffenen auch mit *spezifischen Risiken* verbunden sein (z.B. Furcht vor einer Kündigung des Arbeitsverhältnisses).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

►Gesamtbilanz. Der EDÖB erfüllt seinen gesetzlichen Auftrag und erzielt *im Rahmen seiner Möglichkeiten eine hohe Wirksamkeit*. Die *äusseren Grenzen seiner Wirksamkeit* sind teils gesetzlich und politisch vorgegeben, teils durch die Zunahme intransparenter und grenzüberschreitender Datenbearbeitungen bestimmt und nur schwer beeinflussbar. Aussagen von Interviewpartnern im Rahmen dieser Evaluation zufolge müssen Datenbearbeiter bei einem Verstoss gegen das DSG oft nicht damit rechnen, vom EDÖB zur Rechenschaft gezogen zu werden.

►EDÖB gilt in der Praxis als unabhängig. Im Rahmen der jüngsten Gesetzesrevision (in Kraft seit 1. Dezember 2010) ist die *Unabhängigkeit des EDÖB von der Regierung und der Verwaltung leicht gestärkt* worden, namentlich indem seine Wahl durch den Bundesrat neu vom Parlament genehmigt werden muss. Laut den Aussagen der Interviewpartner sind *in der Praxis des EDÖB bisher nie Zweifel* an seiner Unabhängigkeit gegenüber den staatlichen oder privaten Datenbearbeitern aufgekommen.

► Steuerung des Mitteleinsatzes ziel- und kriteriengeleitet. Obwohl der EDÖB seine Tätigkeit stark auf Anfragen und Meldungen ausrichten muss, die bei ihm vorgebracht werden, versucht er, seine Aktivitäten im Rahmen des Möglichen an *im Voraus hergeleiteten Zielen* auszurichten. Für die Triage und Priorisierung der Geschäfte im Alltag bestehen klare und *aus dem DSG ableitbare Entscheidungskriterien*. Seine Ressourcen verteilt der EDÖB ungefähr ausgewogen auf die *drei Hauptaufgaben* der Aufsicht, der Beratung und der Information respektive der Sensibilisierung.

► Wirksame Aufsichtstätigkeit im Einzelfall. Im Rahmen von Sachverhaltsabklärungen kann der EDÖB *DSG-konforme Datenbearbeitungen sicherstellen*. In der Mehrheit der Sachverhaltsabklärungen stellt er nur geringfügige Probleme fest, welche die Bearbeiter anschliessend freiwillig beheben. Richtet der EDÖB bei grösseren Mängeln *Empfehlungen* an einen Datenbearbeiter, werden diese *grossmehrheitlich umgesetzt*, entweder direkt oder nach einem Gerichtsentscheid.

► Wirksame Beratungs- und Informationstätigkeit im Einzelfall. Die Beratung, die der EDÖB im Einzelfall und auf Anfrage durchführt, wird mit Abstrichen seitens der Bundesorgane von den Bearbeitern insgesamt als *nützlich, praxisnah und konstruktiv* bewertet. Die Qualität der *Publikationen* des EDÖB, die auch als Soft-Law eine gewisse Bedeutung geniessen, beurteilen die befragten Datenbearbeiter und Experten überwiegend als *gut bis sehr gut*. Die zahlreichen Tipps insbesondere an Betroffene greifen häufig jene Themen auf, die sich der Aufsicht entziehen; hier versucht der EDÖB somit, den Selbstschutz zu fördern.

► Grenzen der Aufsichtstätigkeit bei neuen Konstellationen. Die Aufsicht stösst bei Bearbeitungen, die intransparent sind oder im Ausland erfolgen, an ihre Grenzen. Zum einen ist hier die

Wahrnehmbarkeit von Missbräuchen, zum anderen der *Zugriff auf die Bearbeiter* erschwert. Auch die allgemeine Mengenausweitung von Datenbearbeitungen fordert den EDÖB heraus.

► Breitenwirkung der Aufsicht nicht gesichert. Stellt der EDÖB im Rahmen einer Sachverhaltsabklärung bei einem Datenbearbeiter Mängel fest, macht er heute aus Ressourcengründen *bei ähnlichen Bearbeitern keine stichprobenartigen Kontrollen*. Eine präventive Wirkung auf andere Datenbearbeiter entsteht somit allenfalls dort, wo ein Missstand öffentliches Interesse erregt und so sensibilisierend wirkt.

► Begrenzte Inanspruchnahme der Beratung durch Bearbeiter. Der EDÖB wird aufgrund seiner Doppelrolle als Aufsichts- und Beratungsorgan *von einem Teil der Bearbeiter für Beratungen gemieden*, was seine Wirkung als Berater einschränken dürfte.

► Weitere Grenzen der Wirksamkeit. Trotz beachtlicher Nutzungsziffern der Homepage kann insgesamt *nicht von einer breiten direkten Sensibilisierungswirkung* der Informationsangebote ausgegangen werden. *In den Medien ist der EDÖB gut präsent*, allerdings wird die öffentliche Resonanz eines Themas nicht vom EDÖB, sondern von den Medien definiert. Es gibt Hinweise, dass viele *registrierpflichtige Datensammlungen nicht im Register* eingetragen sind, und dass viele *Bearbeitungsreglemente fehlen oder mangelhaft* sind. Die mit diesen Instrumenten bezweckten Wirkungen (mehr Transparenz für die Bevölkerung, Sensibilisierung der Datenbearbeiter) dürften damit nur teilweise erreicht werden. Zu *Gesetzgebungsvorhaben* nimmt der EDÖB konsequent Stellung, wenn er datenschutzspezifische Probleme feststellt. Seine Anpassungsvorschläge werden teilweise berücksichtigt.

Fazit: Wirksamkeit des Gesetzes in Bezug auf vier Referenzgrössen

Insgesamt gehen somit vom DSG klare Wirkungen zugunsten des Datenschutzes aus; gleichzeitig sind die Wirkungen des EDÖB jedoch auch in verschiedener Hinsicht begrenzt, und der Wirkungsmechanismus der Durchsetzungsrechte wird durch die Betroffenen selten genutzt.

Die Frage, ob die Gesamtwirkung des DSG als angemessen zu bewerten ist oder nicht, soll und kann im Rahmen dieser Evaluation nicht abschliessend beantwortet werden. Hierzu fehlt es an klaren Zielvorgaben über das zu erreichende Schutzniveau. Letztlich ist die Antwort auf diese Frage durch die Politik zu geben. Zur *Einordnung der Evaluationsergebnisse* wurde jedoch versucht, die Bestimmungen des DSG und ihre Wirkungen mit vier Referenzgrössen zu vergleichen. An die Befunde der Evaluation anschliessend wurden ferner praktische Empfehlungen abgegeben und Handlungsoptionen skizziert.

► Referenzgrösse 1: Ursprüngliche Erwartungen an das DSG bei Inkrafttreten. Die Evaluation kommt zum Schluss, dass das DSG eine Sensibilisierungs- und Schutzwirkung gezeitigt hat. Diese ist primär auf den Mechanismus des EDÖB zurückzuführen und nur in beschränktem Ausmass auf den Mechanismus der einklagbaren Rechte. Insofern sind die *ursprünglichen Erwartungen ans DSG,* soweit diese überhaupt feststellbar sind, *teilweise erfüllt* worden. Gleichzeitig muss festgehalten werden, dass die bisherigen Instrumentarien des Gesetzes durch die Mengenausweitung an Daten und technologiebedingten Herausforderungen geschwächt und teilweise

ausgehebelt werden, so dass mit einer *tendenziell sinkenden Schutzwirkung* gerechnet werden muss.

► Referenzgrösse 2: Erwartungen von Betroffenen und Bearbeitern. Die Stossrichtung des *DSG nimmt die Grundhaltung sowohl der Bevölkerung als auch der Bearbeiter auf*. Erstere möchte an der Informationsgesellschaft teilnehmen, möchte sich aber auch einer unabhängigen Stelle anvertrauen können, die sie schützt. Während also die Bevölkerung durchaus erwartet, dass der EDÖB seine *Aufsichtsfunktion* wahrnimmt, wünschen sich die Datenbearbeiter von diesem primär *fachliche Unterstützung* bei der Umsetzung der gesetzlichen Vorschriften.

► Referenzgrösse 3: Das DSG im internationalen Rechtsvergleich. Die im DSG verankerten *Durchsetzungsrechte der Betroffenen sind vergleichsweise gut ausgebaut*. Demgegenüber sind die *Kompetenzen des Datenschutzbeauftragten im internationalen Vergleich eher schwach ausgestaltet*.

► Referenzgrösse 4: Verfassungsrechtlicher Mindestschutz. Aufgrund der fehlenden Verfassungsgerichtsbarkeit für Bundesgesetze besteht insbesondere bei Spezialgesetzen, welche eine Datenbearbeitung durch Bundesorgane ermöglichen, trotz verwaltungsinterner Kontrollmechanismen grundsätzlich *keine absolute Garantie*, dass der grundrechtlich garantierte Mindestschutz der Betroffenen gewährleistet ist. Ob, und wenn ja, wie stark dies in der Praxis das Grundrecht auf informationelle Selbstbestimmung einschränkt, wurde im Rahmen dieser Evaluation nicht untersucht.

► Empfehlungen und Handlungsoptionen. Basierend auf den Befunden zu den Aktivitäten des EDÖB gibt die Evaluation einzelne *praktische Empfehlungen* an den EDÖB; diese beziehen sich auf die Dokumentation seiner Aktivitäten und Erfolge sowie auf die Zusammenarbeit mit der Bundesverwaltung. Weiter wurden – ohne Anspruch auf Vollständigkeit – *weiterreichende Handlungsoptionen* skizziert. Diese fussen einerseits in den Befunden der Evaluation und sind andererseits inspiriert von den gegenwärtigen europäischen Reformbestrebungen, die auch die Schweiz tangieren werden. Im Sinne von Gedankenanstössen werden eine Stärkung der Position der Betroffenen in der Auseinandersetzung mit den Datenbearbeitern, eine Stärkung der Aufsichtskompetenzen des EDÖB, eine Stärkung des präventiven Datenschutzes sowie spezifisch auf die technologische Entwicklung ausgerichtete Vorschläge skizziert.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
APPD	Association des Professionnels de la Protection des Données.
AR	Appenzell Ausserrhoden
Art.	Artikel
AS	Amtliche Sammlung des Bundesrechts
ASTRA	Bundesamt für Strassen
AUPER	Automatisiertes Personenregistratursystem
AVAM	Informationssystem für die Arbeitsvermittlung und die Arbeitsmarktstatistik
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BAP	Bundesamt für Polizei (heute fedpol)
BBl	Bundesblatt
BDSG	Bundesdatenschutzgesetz (Deutschland)
BFF	Bundesamt für Flüchtlinge
BFM	Bundesamt für Migration
BFS	Bundesamt für Statistik
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
BGG	Bundesgesetz über das Bundesgericht vom 17. Juni 2005; SR 173.110
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 17. Dezember 2004; SR 152.3
BGr	Bundesgerichtsentscheid (unpubliziert)
BJ	Bundesamt für Justiz
BL	Basel-Landschaft
BPG	Bundespersonalgesetz vom 24. März 2000; SR 172.220.1
BPV	Bundespersonalverordnung vom 3. Juli 2001; SR 172.220.111.3
Bst.	Buchstabe
BSV	Bundesamt für Sozialversicherungen
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
BVerwG	Bundesverwaltungsgericht
BVGE	Bundesverwaltungsgerichtsentscheid
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997; SR 120
CATI	Computer assisted telephone interviewing
CD-ROM	Compact disc read-only memory
CH	Schweiz
CHF	Schweizer Franken
CM	Committee of Ministers (Europarat)
CND	Kanada
CNIL	Commission nationale de l'informatique et des libertés
d.h.	das heisst

DBG	Bundesgesetz über die direkte Bundessteuer vom 14. Dezember 1990; SR 642.11
DE	Deutschland
DNA	Desoxyribonukleinsäure
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992; SR 235.1
DSK	Datenschutzkonvention des Europarates
EDA	Eidgenössisches Aussendepartement
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖK	Eidgenössische Datenschutz- und Öffentlichkeitskommission
EDSB	Eidgenössischer Datenschutzbeauftragter
EDSK	Eidgenössische Datenschutzkommission
EFK	Eidgenössische Finanzkontrolle
EG	Europäische Gemeinschaft (heute: Europäische Union)
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäische Menschenrechtskonvention
EPFL	Ecole Polytechnique Fédérale Lausanne
ES	Spanien
ESOMAR	European Society for Opinion and Marketing Research
ESPOP	Statistik des jährlichen Bevölkerungsstands
etc.	et cetera
EU	Europäische Union
EUV	Vertrag über die Europäische Union
EWR	Europäischer Wirtschaftsraum
F	Frankreich
f.	folgende
FAQ	Frequently asked questions
ff.	Fortfolgende
GASP	Gemeinsame Aussen- und Sicherheitspolitik
GB	Grossbritannien
GE	Genf
ggf.	gegebenenfalls
GPK-N	Geschäftsprüfungskommission des Nationalrats
GPS	Global positioning system
i.c.	in casu
i.d.R.	in der Regel
i.S.	in Sachen
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinn
IDHEAP	Institut de hautes études en administration publique
IP	Internetprotokoll
IT	Informationstechnik, Informationstechnologie
IT	Italien

IV	Invalidenversicherung
KGVVE	Urteil des Kantonsgerichts des Kantons Basel-Landschaft, Abteilung Verfassungs- und Verwaltungsrecht
KMU	Kleine und mittlere Unternehmen
KOM	Dokumente der Kommission (EU)
KVG	Bundesgesetz über die Krankenversicherung vom 18. März 1994; SR 832.10
Loc. cit.	loco citato
m.a.W.	mit anderen Worten
NL	Niederlande
NZZ	Neue Zürcher Zeitung
OGE	Obergericht
OR	Obligationenrecht
ÖS	Österreich
ParlG	Bundesgesetz über die Bundesversammlung (Parlamentsgesetz) vom 13. Dezember 2002; SR 171.10
PC	Personal computer
resp.	respective
Reko	Rekurskommission
RFID	Radio frequency identification
RL	Richtlinie
RRB	Regierungsratsbeschluss
Rz.	Randziffer
SAKE	Schweizerische Arbeitskräfteerhebung
SBB	Schweizerische Bundesbahnen
SECO	Staatssekretariat für Wirtschaft
SH	Schaffhausen
SHAB	Schweizerisches Handelsamtsblatt
SIR	Schweizerisches Institut für Rechtsvergleichung
SIS	Schengener Informationssystem
SIT	Fraunhofer Institut für sichere Informations-Technologie
SL	Slowenien
SR	Systematische Sammlung des Bundesrechts
SUVA	Schweizerische Unfallversicherungsanstalt
T-PD-BUR	Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
u.a.	unter anderem
u.E.	unseres Erachtens
u.v.m.	und viele mehr
UK	Vereinigtes Königreich
Urt. v.	Urteil vom
USA	Vereinigte Staaten von Amerika
UVG	Bundesgesetz über die Unfallversicherung vom 20. März 1981; SR 832.20
v.a.	vor allem
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993; SR 235.11

VGE	Verwaltungsgerichtsentscheide
vgl.	vergleiche
VPB	Verwaltungspraxis der Bundesbehörden (1987–2006)
VPM	Verein für Psychologische Menschenkenntnis
VSMS	Verband Schweizer Markt- und Sozialforscher
VUD	Verein Unternehmensdatenschutz
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968; SR 172.021
VZ	Volkszählung
WEMF	AG für Werbemedienforschung (WEMF)
WTO	World Trade Organization
z.B.	zum Beispiel
z.T.	zum Teil
ZentG	Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes; SR 360
ZG	Zollgesetz
ZGB	Zivilgesetzbuch

TEIL I: EINFÜHRUNG

Dieser Teil enthält eine kurze Einleitung, welche die Ausgangslage der Evaluation und ihren Forschungsgegenstand beschreibt (Kapitel 1). In Kapitel 2 wird die Konzeption der Evaluation vorgestellt. Dazu wird zunächst das Gesetz in seinen Grundzügen erläutert, danach modellhaft seine Wirkungsweise beschrieben und schliesslich das Vorgehen der Untersuchung dargestellt.

1 Einleitung

Dieses Kapitel umreisst die Entwicklung seit dem Inkrafttreten des Datenschutzgesetzes am 1. Juli 1993 und damit die Ausgangslage für die vorliegende Evaluation. Danach wird der Forschungsgegenstand kurz umrissen und eingegrenzt.

1.1 Ausgangslage

Mit der Schaffung eines Datenschutzgesetzes (DSG; SR 235.1) reagierte der Bund anfangs der 1990er Jahre auf die technologiebedingt zunehmend verbesserten Möglichkeiten, Informationen über Personen zu erheben, zu bearbeiten und zu verbreiten. Das neue Gesetz sollte diese Entwicklung nicht verhindern oder einschränken, aber zum Schutz der Persönlichkeit „Leitplanken für die Datenbearbeitung" (Bundesrat/BBl 1988 II 417) setzen. Das Gesetz bezweckt einen stärkeren Schutz vor ungerechtfertigten und unnötigen Datenbearbeitungen (vgl. Art. 3 Bst. e DSG) durch Organe des Bundes und durch Private, und damit eine bessere Wahrung der persönlichen Freiheit und Entfaltung. Jedermann soll, „soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können" (Bundesrat/BBl 1988 II 418). Dieser Grundsatz der „informationellen Selbstbestimmung" wird im Recht als ein Teilgehalt des Grundrechts auf Schutz der Privatsphäre und der Persönlichkeit aufgefasst, das im Völkerrecht (Art. 8 EMRK) und in der Bundesverfassung (Art. 13 Abs. 2 BV) verankert ist.

Das am 1. Juli 1993 in Kraft getretene DSG definiert einerseits einklagbare Grundsätze für Datenbearbeitungen durch Bundesorgane und Private, andererseits legt es die Aufsicht über die Einhaltung dieser Grundsätze und weitere Aufgaben in die Hände eines Datenschutzbeauftragten. Seit dem Inkrafttreten des DSG wurde der Schutz persönlicher Daten durch Schübe der Informationstechnologie sowie durch politische und gesellschaftliche Entwicklungen in den vergangenen beiden Jahrzehnten stark herausgefordert, was nicht nur, aber ganz besonders den Grundssatz der Zweckbindung von Datenbearbeitungen betrifft: „Die Möglichkeiten, dass Daten für andere als die ursprünglichen Zwecke bearbeitet werden und die daraus fliessenden Gefahren bzw. konkreten Persönlichkeitsverletzungen sind durch die heute zur Verfügung stehenden modernen Informationssysteme und die verlockende Verfügbarkeit einer immensen Datenmenge stark gestiegen" (Maurer-Lambrou/Steiner 2006: 82).

Das Datenschutzgesetz hat bis 2010 mehrere Änderungen erfahren: 2006 wurde der Tätigkeitsbereich des Datenschutzbeauftragten um das Öffentlichkeitsgesetz (BGÖ; vgl. Bundesrat/BBl 2003a: 1963-2046) erweitert. Am 1. Januar 2008 trat eine Teilrevision des DSG in Kraft (Bundesrat 2003b: 2101-2155), und in Zusammenhang mit der Umsetzung des Rahmenbeschlusses der EU über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, wurde u.a. das Verfahren zur Wahl des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geändert. Diese Reform,

die mit dem Beitritt der Schweiz zu den Abkommen von Schengen und Dublin zusammenhängt, trat am 1. Dezember 2010 in Kraft (vgl. Bundesrat/BBl 2009: 6749-6786).

Trotz dieser punktuellen Anpassungen bleiben der Datenschutz und das Instrumentarium seiner Durchsetzung jedoch laut der neusten juristischen Literatur teilweise noch mit Mängeln behaftet, so z.B. bei den Aufsichts- und Sanktionskompetenzen des EDÖB, bei der Haftpflicht von Privaten, im Verfahrensrecht, beim Zugang zu den eigenen Daten, bei den Informationspflichten der Datenbearbeiter oder beim Transfer von Daten ins Ausland (vgl. Schweizer 2009; Menétrey-Savary 2009: 153-154). Auch politische Vorstösse verlangen teilweise neue Instrumente zur Stärkung des Datenschutzes. Umgekehrt wurde in der öffentlichen Diskussion aber auch vor unzumutbaren Efforts für die Datenbearbeiter und zu grossen Hindernissen der Datenbearbeitung durch die Anforderungen des Datenschutzes gewarnt und z.B. der politische Druck erhöht, den Datenaustausch zwischen Behörden zu erleichtern, so u.a. um Leistungsmissbräuche in der Sozialversicherung bessern bekämpfen zu können (vgl. Bolliger/Féraud 2010; Bundesrat 2010).

Während das Datenschutzrecht in der juristischen Literatur breit diskutiert wird, gibt es kaum empirische Studien zur Umsetzung und den tatsächlichen Wirkungen des Gesetzes. Ausnahmen bilden eine Untersuchung der nationalrätlichen Geschäftsprüfungskommission zum Datenschutz in der Bundesverwaltung (GPK-N 2003; Bundesrat/BBl 2004: 1431-1436), eine Analyse der Eidgenössischen Finanzkontrolle beim EDÖB (EFK 2007) sowie eine Untersuchung zum Datenaustausch zwischen Behörden (Bolliger/Féraud 2010; Bundesrat 2010). Zum Umgang der Betroffenen mit ihren persönlichen Daten, ihren Einstellungen zum Datenschutz und zum Informationsaustausch sowie zu ihren Kenntnissen und Erfahrungen bezüglich des DSG gibt es in der Schweiz erst eine Umfrage (Privatim 2009).

Vor diesem Hintergrund hat das Bundesamt für Justiz (BJ) eine Gesamtevaluation des Datenschutzgesetzes ausgeschrieben und der Büro Vatter AG, dem Institut für Europarecht der Universität Freiburg und dem Umfrageinstitut Demoscope AG den Auftrag zur Evaluation der Wirksamkeit des DSG erteilt. Die Projektleitung lag beim Büro Vatter. Die Evaluation wurde von der Arbeitsgruppe Evaluation DSG, bestehend aus Mitgliedern der Verwaltung, einer Vertretung des EDÖB, Experten und Interessenvertretern begleitet (vgl. Anhang 5). Ergänzend hat das BJ das Schweizerische Institut für Rechtsvergleichung (SIR), Lausanne, mit einer Länder vergleichenden Studie über zentrale Aspekte des Datenschutzrechts beauftragt. Deren Ergebnisse fliessen in zusammengefasster Form in den vorliegenden Evaluationsbericht ein. Die Arbeiten an der Evaluation dauerten von Mai 2010 bis Februar 2011.

1.2 Ziel und Gegenstand der Evaluation

Ziel der Evaluation ist es, verschiedene Teilaspekte des DSG hinsichtlich ihrer Effektivität, ihrer Wirksamkeit und ihrer Effizienz zu überprüfen und gegebenenfalls Vorschläge für Anpassungen im Vollzug oder in den gesetzlichen Bestimmungen zu machen. Nicht Gegenstand der Evaluation sind die im Zuge der Reformen des DSG per 1.1.2008 und 1.12.2010 eingeführten neuen Bestimmungen, weil hierzu noch zu wenige Erfahrungen vorliegen.

Im Vordergrund der Evaluation stehen erstens die Bekanntheit und die Durchsetzungsmechanismen des Gesetzes; dabei ist von besonderem Interesse, welche Rechtsansprüche und Verfahren, welche das DSG den betroffenen Personen zur Verfügung stellt, sich als wirksam erwiesen haben, und damit geeignet sind, den Schutz der Persönlichkeit und der Grundrechte angemessen zu gewährleisten.

Der zweite Schwerpunkt befasst sich mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB[1]). Untersucht werden soll, welchen Stellenwert dem EDÖB zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen zukommt. Dabei sind seine institutionelle Stellung und Unabhängigkeit, seine Organisation und die Wirksamkeit seiner Aktivitäten zu untersuchen. Aufgrund der Fragestellungen, der zur Verfügung stehenden Informationsquellen und der Ressourcen liegt dabei der Fokus stärker auf der strategischen Ebene des EDÖB-Handelns und den strukturellen Grenzen seiner Wirksamkeit als auf der praktischen Umsetzung seiner Strategie und der Abläufe im Arbeitsalltag.

Die Evaluation erfolgt vor dem Hintergrund der technologischen Entwicklungen seit dem Inkrafttreten des DSG und der damit verbundenen neuen Herausforderungen für den Datenschutz. Zu berücksichtigen sind dabei die Verhaltensweisen und Erfahrungen der Datenbearbeiter und der Personen, die von Datenbearbeitungen betroffen sind.

Im Vordergrund der Evaluation steht somit das Datenschutzgesetz des Bundes und nicht das Gesamtsystem des Datenschutzes in der Schweiz, das gewisse Kompetenzen und Zuständigkeiten den Kantonen zuschreibt. Die Aufgabenteilung, die Schnittstellen und die Koordination zwischen Bund und Kantonen im Bereich des Datenschutzes werden hier somit nur am Rand berücksichtigt. Auch die Möglichkeiten der internationalen Zusammenarbeit von Behörden im Zusammenhang mit dem Datenschutz stehen nicht im Mittelpunkt der Untersuchung, ebenso wenig wie die Praxis und das Funktionieren der Meldepflicht bei Datenbekanntgaben ins Ausland (Art. 6). Auch zum Datenaustausch zwischen den Behörden im Zusammenhang mit der Verhinderung von Missbräuchen z.B. im Sozialbereich äussert sich diese Evaluation nicht; es kann diesbezüglich auf die Studie Bolliger/Féraud (2010) und den entsprechenden Bericht des Bundesrats (2010) verwiesen werden.

[1] Wenn in diesem Bericht der Begriff „EDÖB“ ohne nähere Umschreibung verwendet wird, so ist die Behörde als ganzes gemeint, und nicht die Person des Beauftragten selbst. Hierzu wird der Begriff „Beauftragter“ oder „Chef EDÖB“ verwendet. Personen beim EDÖB, die im Rahmen von Interviews befragt wurden, werden unabhängig von Ihrer Stellung innerhalb der Organisation als „Mitarbeitende des EDÖB“ bezeichnet.

2 Konzeption der Untersuchung

Dieses Kapitel bildet die Grundlage für die folgenden Teile der Evaluation, die sich empirisch mit der Umsetzung und der Wirksamkeit des DSG befassen werden. Ein erster Abschnitt stellt das schweizerische Datenschutzgesetz in seinen Grundzügen vor und untersucht ergänzend, inwiefern die Grundsätze des schweizerischen Rechts auch in anderen Ländern verankert sind. Weitere Inhalte des DSG (Durchsetzungsrechte für die Betroffenen, Aufsichtsorgan) werden im Rahmen der empirischen Teile dieser Untersuchung behandelt. Daran anschliessend wird das Modell über die Wirkungsweise des Datenschutzgesetzes hergeleitet, das dieser Untersuchung zugrunde liegt: Dazu wird der Begriff der Datenschutzsensibilität der Betroffenen und Datenbearbeiter eingeführt, sowie die Wirkungsmechanismen des DSG und wichtige Kontextfaktoren erörtert. Im letzten Abschnitt wird das Vorgehen der Evaluation erläutert.

2.1 Die Grundzüge des schweizerischen Datenschutzgesetzes

Nachfolgend werden zunächst der Zweck und die Grundbegriffe des DSG erläutert, bevor die Grundsätze des Datenschutzgesetzes vorgestellt und mit denjenigen anderer Länder verglichen werden. Auch auf die Reichweite und das Verhältnis zu anderen datenschutzrelevanten Gesetzen des DSG ist einzugehen

2.1.1 Zweck des Datenschutzgesetzes

Das Datenschutzgesetz konkretisiert den grundrechtlichen Schutz der Privatsphäre, wie er in Art. 8 Abs. 1 EMRK sowie in der Bundesverfassung verankert ist. Art. 13 Abs. 2 BV legt fest: „Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten." Obwohl es aus dem Wortlaut der Norm nicht klar hervorgeht, wird mit dieser Bestimmung das Grundrecht auf informationelle Selbstbestimmung definiert. Damit wird ein Schutzniveau hinsichtlich der persönlichen Daten statuiert, das nur unter den Voraussetzungen von Art. 36 BV eingeschränkt werden kann, d.h. die Einschränkung muss auf einer gesetzlichen Grundlage beruhen, ein öffentliches Interesse oder den Schutz von Grundrechten Dritter bezwecken sowie den Grundsatz der Verhältnismässigkeit und den Kerngehalt des Grundrechts auf informationelle Selbstbestimmung wahren. Dem Recht auf informationelle Selbstbestimmung kommt horizontale Drittwirkung zu, d.h. eine Schutzpflicht besteht auch gegenüber Datenbearbeitungen durch Privatpersonen. Konkretisiert wird dieser Schutzbereich durch Art. 4 ff. und Art. 12 ff. DSG (Schweizer 2008: 326 (N. 43) zu Art. 13).

Das DSG bezweckt gemäss Art. 1 „den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden". Der Schutz der Persönlichkeit zielt dabei primär auf die Bearbeitungen durch Private, der Schutz der Grundrechte auf die Bearbeitungen durch staatliche Behörden.

Zur Motivation des Datenschutzes führte der Bundesrat in seiner Botschaft an, der Umgang mit Daten könne sich in verschiedener Weise nachteilig oder verletzend auf die betroffene Person

auswirken: Verunsicherung, wenn man nicht mehr überblickt, wer Daten über einem bearbeitet; Anmassung durch indiskretes Auskunftschaften; Benachteiligung oder unbillige Behandlung aufgrund unrichtiger, unvollständiger oder nicht mehr aktueller Informationen; lebenslänglicher Makel aufgrund dauerhafter Aufbewahrung und Verwendung negativer Angaben; Verletzung der Persönlichkeit durch übermässiges Bearbeiten, z.B. durch Anprangern in der Öffentlichkeit oder Erheben unnötiger Angaben bei einem Vertrag; Verletzung durch Zweckentfremdung der Daten (Bundesrat 1988: BBl 1988 II 416).

Das DSG will somit verhindern, dass Personen durch nicht konformes Bearbeiten ihrer Daten einen Schaden erleiden; sie sollen also zum Beispiel nicht aufgrund bestimmter Informationen, die ein Arbeitgeber nicht ohne Wissen der Person beschaffen dürfte, ihre Stelle verlieren. Das DSG setzt aber bereits vor dem Schaden an, indem es – anknüpfend an den grundrechtlichen Schutz der Privatsphäre – die Personen generell vor einer informationellen Entblössung schützen will.

Dabei ist es nicht die Absicht des Gesetzgebers, mit dem DSG Datenbearbeitungen generell zu unterbinden; vielmehr sollten diese so ausgestaltet werden, dass der informationellen Selbstbestimmung Genüge getan wird: „Ein Datenschutzgesetz hat nicht den Zweck, die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken." Vielmehr seien „gewisse Leitplanken für die Datenbearbeitung zu setzen, die garantieren, dass die Entfaltung der Persönlichkeit nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird" (BBl 1988 II 417-418).

2.1.2 Grundbegriffe des Datenschutzgesetzes

Das Gesetz bezieht sich auf das Bearbeiten von *Personendaten*, also von „Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen" (Art. 3 Bst. a). Gewisse Personendaten unterstehen einem qualifizierten Schutz. Dazu zählen erstens besonders schützenswerte Personendaten (Art. 3 Bst. c), so Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Tätigkeiten, Daten über die Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Daten über Massnahmen der sozialen Hilfe sowie Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Zweitens zählen dazu Persönlichkeitsprofile (Art. 3 Bst. d). Dabei handelt es sich um eine „Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt." Natürliche oder juristische Personen, von denen Personendaten bearbeitet werden, werden in diesem Bericht als *Betroffene* oder als *betroffene Personen* bezeichnet. Bundesorgane sowie private natürliche oder – was meist der Fall sein dürfte – juristische Personen, die Daten bearbeiten, werden als *Datenbearbeiter* oder als *Bearbeiter* bezeichnet.

Als *Datenbearbeitung* (Art. 3 Bst. e und f) gilt jeder Umgang mit Personendaten, so insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben (d.h. zugänglich Machen, Einsicht Gewähren, Weitergeben, Veröffentlichen), Archivieren oder Vernichten von Daten.

2.1.3 Datenschutzgrundsätze, Rechte und Pflichten im schweizerischen DSG

Die Grundsätze der Datenbearbeitung sind in Art. 4 DSG festgeschrieben. Sie definieren positiv, welche Verhaltensweisen beim Bearbeiten von Daten zulässig sind und legen damit fest, „dass wer gegen die Grundsätze verstösst, die Persönlichkeit der betroffenen Person verletzt" (Rosenthal/Jöhri 2008: 77):

- *Rechtmässigkeit (Abs. 1):* Die Persönlichkeit wird verletzt, wenn die Bearbeitung der persönlichen Daten auf einem unrechtmässigen Verhalten beruht, d.h. wenn dieses gegen eine Norm der Schweizer Rechtsordnung verstösst, ohne dass dies durch eine vorrangige Gegennorm erlaubt wird. Ein Beispiel dafür ist die Beschaffung von Daten durch Arglist, Gewalt oder Drohung, also eine Verletzung des Strafgesetzbuches.

- *Treu und Glauben (Abs. 2):* Der Grundsatz legt fest, dass Datenbearbeitungen nur so vorgenommen dürfen, wie von einem redlich und anständig handelnden Menschen erwartet werden kann. So verstösst z.B. die heimliche Datenbearbeitung gegen diesen Grundsatz.

- *Verhältnismässigkeit (Abs. 2):* Personendaten dürfen nur soweit bearbeitet werden, als dies für einen bestimmten Zweck objektiv geeignet und erforderlich ist. So ist etwa das Sammeln von Daten auf Vorrat nicht verhältnismässig. Weiter muss die Bearbeitung für die betroffne Person sowohl hinsichtlich ihres Zwecks als auch ihrer Mittel zumutbar sein. Der Verhältnismässigkeitsgrundsatz bestimmt in konkreten Entscheidungssituationen somit nicht nur, welche Art von Daten bearbeitet werden dürfen, sondern auch „in welcher Quantität, in welcher Qualität, in welcher Häufigkeit, zu welcher Zeit, wie lange, auf welche Weise, von welchen Personen, durch welche Personen, an welchen Orten sowie jeden anderen Aspekt der Bearbeitung von Personendaten" (Rosenthal/Jöhri 2008: 86).

- *Zweckbindung (Abs. 3):* Personendaten dürfen nur zu jenem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

- *Erkennbarkeit (Abs. 4):* Für die betroffene Person muss es erkennbar sein, wenn von ihr Personendaten beschafft werden. Der Grundsatz begründet an sich keine Informationspflicht, wenn die Beschaffung und insbesondere ihr Zweck für den Betroffenen aus den Umständen ersichtlich sind, kann aber eine Information je nach Situation erfordern.

Diese Grundsätze gelten nicht absolut. Wenn der Datenbearbeiter einen Rechtfertigungsgrund hat, ist die Verletzung nicht widerrechtlich, wobei für private Bearbeiter und für Bundesorgane teilweise unterschiedliche Rechtfertigungsgründe gelten. Festzuhalten ist, dass die im DSG aufgeführten Grundsätze insoweit deklamatorischen Charakter haben, als gewisse Prinzipien unabhängig vom DSG ohnehin gelten. Dies gilt insbesondere für die Grundsätze von Treu und Glauben und der Rechtmässigkeit. Der Verhältnismässigkeitsgrundsatz gilt unabhängig vom DSG ohnehin für das Handeln von Bundesorganen; für Datenbearbeitungen von Privaten entfaltet seine Verankerung im DSG jedoch eine Rechtswirkung. Die Zweckbindung und die Erkennbarkeit sind spezifische Grundsätze des Datenschutzrechts.

Über die Verpflichtungen hinaus, die sich aus den Grundsätzen des DSG ergeben, präzisiert das DSG die Rechte und Pflichten von Datenbearbeitern und Betroffenen in weiteren Bestimmungen. So hat der Bearbeiter eine weit gehende Verantwortung über die Richtigkeit der Daten (Art. 5 DSG) und er muss Daten durch angemessene technische und organisatorische Massnahmen vor unbefugtem Bearbeiten schützen, was im Begriff der Datensicherheit zusammengefasst wird (Art. 7 DSG). Art. 7a bis 10 DSG umschreiben die Informationspflicht des Datenbearbeiters bei besonders schützenswerten Daten und Persönlichkeitsprofilen sowie das Recht der Betroffenen auf Auskünfte über Datenbearbeitungen.

Sämtliche Datensammlungen der Bundesorgane müssen im Register der Datensammlungen angemeldet sein, bevor sie eröffnet werden (Art. 11a DSG). Dasselbe gilt für Datensammlungen von Privaten, wenn regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden, oder wenn regelmässig Personendaten an Dritte bekannt gegeben werden. Diverse Ausnahmen sind vorgesehen.

Für die grenzüberschreitende Bekanntgabe von Personendaten hat der Gesetzgeber besondere Regeln aufgestellt, weil sich je nach Datenschutzniveau des Ziellandes durch die Bekanntgabe besondere Gefährdungen ergeben können. Art. 6 Abs. 1 DSG formuliert ein grundsätzliches Verbot der grenzüberschreitenden Bekanntgabe, wenn durch die Bekanntgabe die Persönlichkeit der Betroffenen „schwerwiegend" gefährdet würde, namentlich, wenn ein genügender gesetzlicher Schutz fehlt; Art. 6 Abs. 2 DSG enthält die dazugehörigen Ausnahmebestimmungen.

2.1.4 Verhältnis des DSG zu anderen datenschutzrechtlichen Bestimmungen

Das DSG ist anwendbar, wenn Bundesorgane oder natürliche oder juristische private Personen Daten von natürlichen und juristischen Personen bearbeiten (Art. 2 Abs. 1 DSG). Privatpersonen, die mit öffentlichen Aufgaben des Bundes betraut sind (z.B. Krankenversicherungen in der obligatorischen Grundversicherung) gelten dabei als Bundesorgane (Art. 3 Buchstabe h DSG). Umgekehrt gelten Bundesorgane bei der Ausübung privatrechtlicher Tätigkeiten als Privatpersonen.

Verhältnis zum kantonalen Recht: Datenbearbeitungen von kantonalen oder kommunalen Behörden unterstehen dem kantonalen Recht. Das DSG verpflichtet die Kantone, ein Datenschutz-Kontrollorgan einzusetzen (Art. 37 Abs. 2 DSG). Die Datenbearbeitung durch kantonale Behörden fällt auch dann nicht unter das DSG, wenn diese Behörden Bundesaufgaben vollziehen, weil die Bundesverfassung dem Bund keine umfassende Kompetenz zur Regelung des Datenschutzes erteilt. Wenn keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten, gelten jedoch für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht gewisse Bestimmungen des DSG (Art. 37 Abs. 1 DSG). Der Bund kann jedoch in jenen Sachbereichen den Datenschutz „mitregeln", wo ihm eine entsprechende Sachkompetenz erteilt wird („Annexkompetenz"; Epiney/Civitella/Zbinden 2009: 18[2]). Der EDÖB unterstützt neben den Bundesorganen auch solche der Kantone in Fragen des Datenschutzes (Art. 31 Abs. 1 Bst. a DSG).

[2] Zur Regelungskompetenz des Bundes vgl. auch Rudin 2006: 489ff..

Verhältnis zum internationalen Datenschutzrecht: Im internationalen Recht bildet wie erwähnt Art. 8 EMRK die massgebliche grundrechtliche Basis für das schweizerische DSG. Die am 17.9.1980 unterzeichnete und am 1.10.1985 in Kraft getretene und auch durch die Schweiz ratifizierte Konvention Nr. 108 des Europarats zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten formuliert für die Vertragsparteien einen verbindlichen datenschutzrechtlichen Mindeststandard. Die Schutzwirkungen der Konvention wurden später durch das von der Schweiz ratifizierte Zusatzprotokoll Nr. 181 verstärkt (Epiney/Civitella/Zbinden 2009: 11). Derzeit sind Bestrebungen in Gange, die Konvention Nr. 108 zu modernisieren (vgl. Ziffer 15.3.).

Verhältnis zum EU-Recht: Mit dem Beitritt zu den Abkommen von Schengen und Dublin hat sich die Schweiz zur Übernahme der diesbezüglichen rechtlichen Vorgaben der EU an den Datenschutz verpflichtet. Hierzu gehören die relevanten sektoriellen Bestimmungen insbesondere im Bereich der polizeilichen Zusammenarbeit und Eurodac, aber auch die EG-Datenschutzrichtlinie 95/46 (Epiney/Civitella/Zbinden 2009: 15-16). Am 1. Dezember 2010 ist die entsprechende neueste DSG-Teilrevision in Kraft getreten; dabei wurde das DSG an die Vorgaben des Rahmenbeschlusses 2008/977 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen angepasst (vgl. dazu das Bundesgesetz über die Umsetzung des Rahmenbeschlusses 2008/977 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen; AS 2010 3387). Auch in der EU sind Reformbestrebungen im Gange (vgl. Ziffer 15.3).

Verhältnis zu Spezialrecht des Bundes: Das DSG ist ein Rahmengesetz. Es legt Anforderungen an Datenbearbeitungen in den Datenschutzgrundsätzen fest, und es sieht Institutionen und Verfahren (Gericht, EDÖB) vor, die die Einhaltung dieser Grundsätze sicherstellen sollen. Wie Datenbearbeitungen konkret ausgestaltet werden sollen, ist jedoch im konkreten Einzelfall zu regeln. Datenbearbeitungen von Bundesorganen müssen sich gemäss dem Legalitätsprinzip auf eine Rechtsgrundlage stützen. Spezialrechtliche Bestimmungen enthalten somit Regelungen, welche die zulässigen Datenbearbeitungen eines Bundesorgans im Rahmen seiner Aufgabenerfüllung umschreiben. Auch in gewissen privatrechtlichen Tätigkeiten gibt es zusätzliche gesetzliche Grundlagen, welche den Umgang mit persönlichen Daten regeln, so etwa das Bankkundengeheimnis oder das Arztgeheimnis.

2.1.5 Grundsätze der Datenbearbeitung im internationalen Vergleich

Im internationalen Rechtsvergleich (vgl. Ziffer 2.3) zeigt sich hinsichtlich der Grundsätze der Datenbearbeitung eine hohe Übereinstimmung. Diese hängt stark mit dem bestehenden Gemeinschaftsrecht der EU zusammen, insbesondere mit der Richtlinie 95/46 (Art. 6 RL 94/95). Diese hat „eine umfassende Rechtsharmonisierung herbei geführt und auch über die Grenzen des EWR die Rechtsentwicklung beeinflusst, so insbesondere in Kanada“ (SIR 2010: 11). Sämtliche berücksichtigten Staaten kennen sowohl die Prinzipien der Rechtmässigkeit, der Verhältnismässigkeit sowie der Zweckbindung. Das Prinzip von Treu und Glauben ist in Frankreich (unter dem Begriff der „loyauté“), den Niederlanden, Österreich, Grossbritannien, Kanada und Slowenien verankert, nicht aber in Deutschland, Italien und Spanien. Das deutsche Datenschutzgesetz setzt

anstelle des Grundsatzes von Treu und Glauben auf den Grundsatz des Verbots (von Bearbeitungen) mit Erlaubnisvorbehalt. Bearbeitungen sind erlaubt, wenn eine gesetzliche Grundlage besteht oder die Einwilligung vorliegt. Anders als die Schweiz hat Deutschland den Grundsatz der Datenvermeidung und der Datensparsamkeit im Gesetz festgehalten. Dieser zielt darauf ab, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

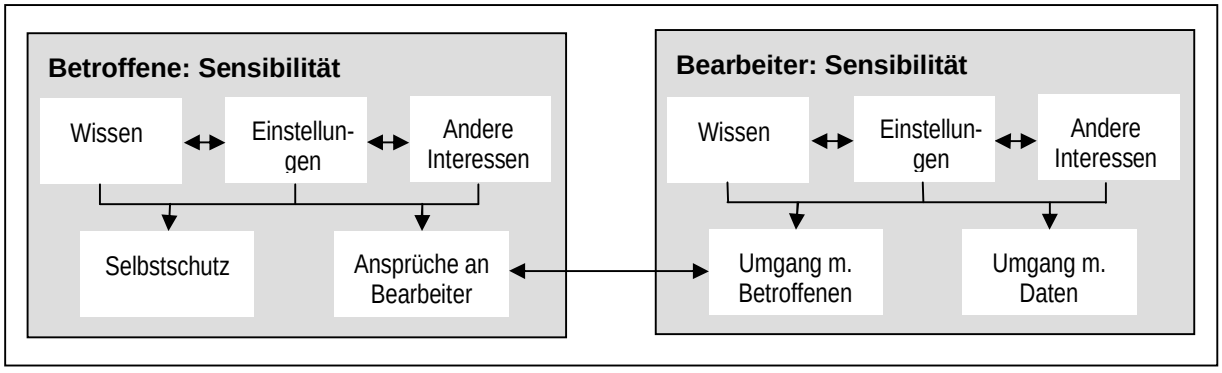
2.2 Sensibilität der Akteure und Wirkungsweise des DSG

Nachdem die Grundzüge des Gesetzes vorgestellt worden sind, soll in diesem Abschnitt seine vom Gesetzgeber beabsichtigte Wirkungsweise erörtert werden. Hierzu wird das Wirkungsmodell hergeleitet, das dieser Untersuchung zugrunde liegt. Zunächst ist ein Blick auf die wichtigsten Akteure im Bereich des Datenschutzes zu werfen: die Datenbearbeiter und die Betroffenen. Im Zentrum steht dabei der Begriff der Datenschutzsensibilität. Hernach werden die Wirkungsmechanismen und die beeinflussenden Kontextfaktoren des DSG beschrieben. Dieses Kapitel bildet die konzeptionelle Grundlage für die in den Teilen II, III und IV präsentierten empirischen Befunde.

2.2.1 Sensibilität für den Datenschutz

Abbildung 2-1 veranschaulicht modellhaft die Eigenschaften der Betroffenen und der Datenbearbeiter, die wir jeweils unter dem Begriff der *Datenschutzsensibilität* oder abgekürzt *Sensibilität* zusammenfassen. Diese Sensibilität umfasst Einstellungs-, Wissens- und Verhaltenskomponenten.

Abbildung 2-1: Beziehung von Datenbearbeitern und Betroffenen



Sensibilität der Betroffenen für den Datenschutz

Das Modell geht davon aus, dass die Betroffenen über bestimmte – individuelle und im Zeitlauf variable –Einstellungen zum Schutz ihrer persönlichen Daten verfügen. Vereinfacht gesagt: Der Datenschutz kann ihnen prinzipiell wichtig oder unwichtig sein. Gleichzeitig verfolgen die Betroffenen auch andere Interessen. Häufig tangieren diese Interessen den Datenschutz nicht. Es gibt aber Situationen, in denen diese Interessen und der Wunsch nach Privatsphäre kollidieren. So müssen Personen z.B. beim Kauf bestimmter Dienstleistungen ihre Identität bekannt geben,

oder sie möchten in Sozialen Netzwerken im Internet Informationen austauschen, die für einen zu definierenden Personenkreis ersichtlich sind. Es ist davon auszugehen, dass die Betroffenen auch über ein unterschiedlich gutes Wissen über mögliche Bedrohungen ihrer Privatsphäre durch Datenbearbeiter, über ihre Rechte und über mögliche Abwehrreaktionen verfügen. Es ist ferner anzunehmen, dass die Einstellungen und das Wissen bis zu einem gewissen Grad zusammenhängen: Personen, denen der Datenschutz wichtig ist, dürften motivierter sein, sich entsprechendes Wissen über die Möglichkeiten des Selbstschutzes, über die Bearbeiter, aber auch über ihre Rechte anzueignen. Umgekehrt kann vermutet werden, dass informierte Personen dem Datenschutz eine höhere Priorität einräumen.

Aus der Kombination des Wissens, der Einstellungen und den anderen, potenziell konkurrierenden Interessen der Personen ergibt sich im Modell das datenschutzbezogene Verhalten der betroffenen Personen. Es umfasst zwei Dimensionen: Zum einen können Personen ihre informationelle Selbstbestimmung wahrnehmen, indem sie bewusst entscheiden, welche Daten sie bekannt geben und welche Schutzmassnahmen vor Zugriffen unbefugter Dritter sie ergreifen. Diese Verhaltensdimension wird als Selbstschutz bezeichnet. Zum anderen können sie die informationelle Selbstbestimmung wahrnehmen, indem sie bei den Datenbearbeitern ihre Ansprüche geltend machen, zum Beispiel indem sie Informationen darüber verlangen, wozu die gelieferten Daten verwendet werden. Hierzu definiert das Datenschutzgesetz bestimmte Ansprüche.

Sensibilität der Datenbearbeiter für den Datenschutz

Bei den Datenbearbeitern kann ebenfalls ein bestimmtes – und individuell unterschiedliches – Niveau der Sensibilität für Fragen des Datenschutzes angenommen werden. Auch bei den Bearbeitern konkurrenziert diese Sensibilität potenziell mit anderen Interessen. So verfolgen Privatunternehmen kommerzielle Zwecke, zu deren Erreichung bisweilen Datenbearbeitungen notwendig oder zumindest hilfreich sind. Beispiele sind das Sammeln von Adressdaten zur Pflege eines Kundenstamms oder die Auswertung des Kaufverhaltens von Kunden für zielgerichtete Werbung. Bundesorgane verfolgen ebenfalls Zwecke, für die Datenbearbeitungen hilfreich und notwendig sein können, so etwa die Überwachung von Personen zur Gewährleistung der inneren Sicherheit oder das Auswerten von Personendaten aus Registern und Umfragen für statistische Zwecke.

Auch bei den Bearbeitern können unterschiedliche Einstellungen und ein unterschiedliches Wissen zu Datenschutzfragen vermutet werden, das sich z.B. im unterschiedlichen Ausbaugrad von betriebsinternen Datenschutzstrukturen und -prozessen manifestieren dürfte. Es lassen sich zwei Verhaltenskomponenten unterscheiden: Zum Umgang mit den Daten gehören alle Aktivitäten, die sich unmittelbar mit der Bearbeitung von Daten und ihrer sicheren Aufbewahrung befassen. Zum Umgang mit den Betroffenen gehören alle Aktivitäten, die der Bearbeiter unternimmt, um die Rechte der Betroffenen zu schützen (Information, Einholen von Einwilligungen, etc.).

Aus den jeweiligen Niveaus der Sensibilität für den Datenschutz bei den Betroffenen und den Bearbeitern ergibt sich, wie intakt die Beziehung zwischen den beiden Akteursgruppen und wie gut der Datenschutz insgesamt funktioniert. Wenn die Bearbeiter über eine hohe Sensibilität für den Datenschutz verfügen, kann erwartet werden, dass unabhängig von der Sensibilität der Be-

troffenen ein hohes Schutzniveau erreicht wird. Die Beziehung zwischen den beiden Gruppen kann als intakt bezeichnet werden.

Wenn sowohl die Betroffenen wie die Bearbeiter über eine tiefe Sensibilität verfügen, so dürfte zwar zunächst eine intakte Beziehung zwischen den Akteursgruppen bestehen, jedoch ist das Datenschutzniveau hier tief. Es besteht das Risiko, dass die Rechte der Betroffenen ohne ihr Wissen verletzt werden; spätestens wenn eine Person zu Schaden kommt und dies merkt, dürfte die Beziehung (zumindest auf individueller Ebene) nicht mehr intakt sein.

Wenn die Sensibilität der Bearbeiter tief, jene der Betroffenen aber hoch ist, ist die Beziehung nicht mehr intakt. Die Betroffenen stellen in diesem Fall höhere Ansprüche an die Bearbeiter als diese zu gewährleisten bereit sind. Es kommt zu Konflikten und es stellt sich die Frage, ob sich der Betroffene oder der Bearbeiter durchsetzen.

2.2.2 Wirkungsmechanismen des Datenschutzgesetzes und Kontext

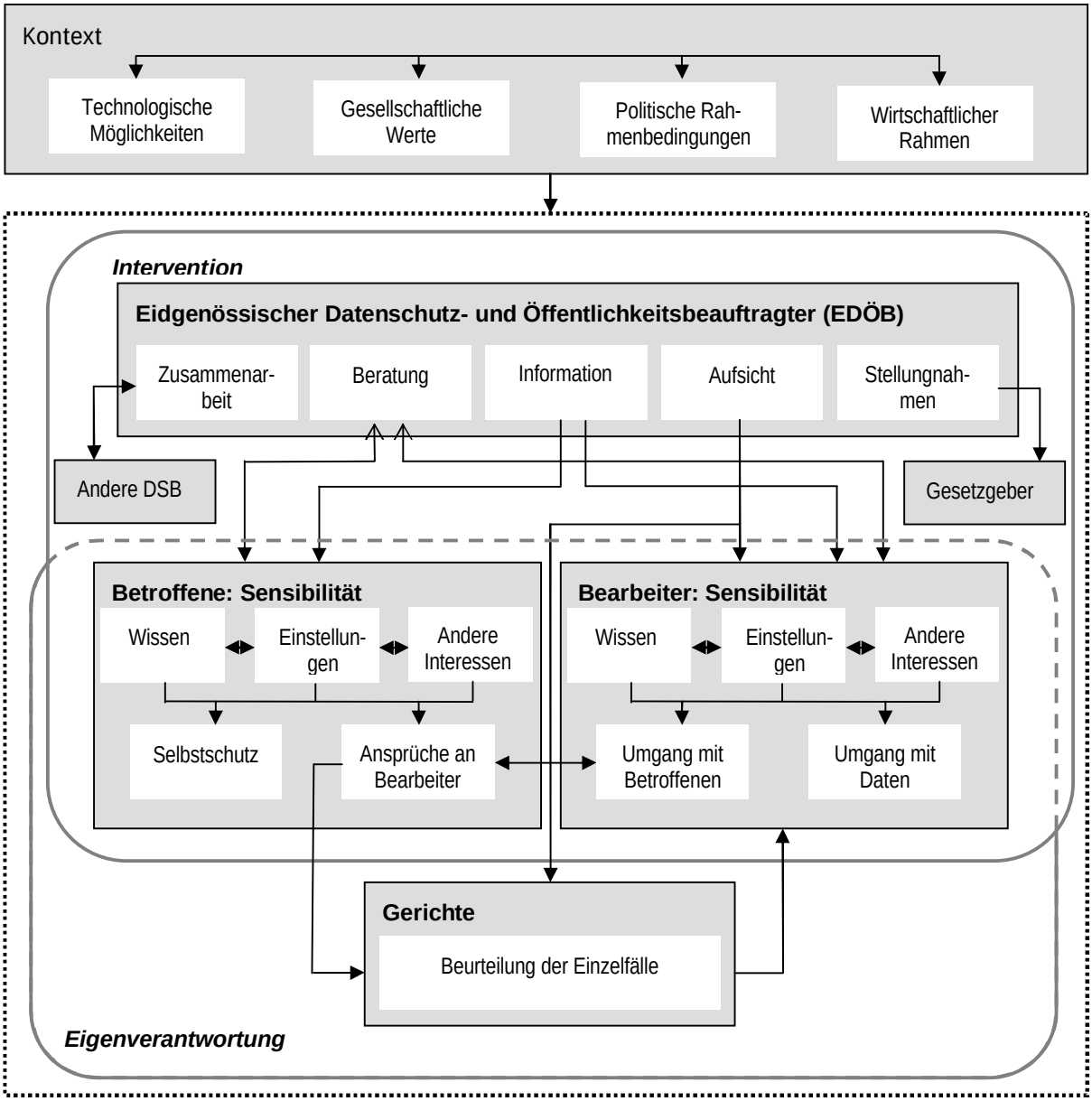
Das Datenschutzgesetz greift hauptsächlich mit zwei Strategien in die Sensibilität und die Beziehungen zwischen den Betroffenen und den Bearbeitern ein: Das Gesetz sieht erstens den Wirkungsmechanismus des Rechtswegs vor. Zweitens sieht es den Wirkungsmechanismus über den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vor (Abbildung 2-2).

Wirkungsmechanismus des Rechtswegs

Der Wirkungsmechanismus des Rechtswegs beruht auf dem Prinzip der Eigenverantwortung der Betroffenen. Ihnen wird ermöglicht, ihre Rechte gerichtlich geltend zu machen, wenn sie diese verletzt glauben und der Bearbeiter ihrem Begehren nicht nachkommt. Zu diesen Rechten gehören das Recht auf Auskunft über Bearbeitungen (Art. 8 DSG) und die Durchsetzungsrechte, mit denen in eine Bearbeitung eingegriffen werden kann (Art. 15 und 25 DSG). Gerichtsurteile wirken zum einen direkt im Einzelfall, indem sie den Bearbeiter zur Anpassung seiner Praxis zwingen. Gleichzeitig haben Gerichtsentscheide gelegentlich den Charakter von Leiturteilen, indem sie die gesetzlichen Bestimmungen konkretisieren. Diese Urteile entfalten potenziell auch eine Breitenwirkung.

Dass Betroffene den Rechtsweg einschlagen können, bedingt ein Mindestmass an Sensibilität und Wissen, einerseits über die Bearbeitungen, andererseits über die bestehenden Rechte, die Rechtsmittel und ihre Anwendung. Eine hohe Zahl an (erfolgreichen) Klagen lässt auf eine hohe Sensibilität und eine tiefe Sensibilität bei den Bearbeitern, oder zumindest auf eine gewisse Unzufriedenheit bei den Betroffenen schliessen. Eine tiefe Zahl an Klagen lässt auf eine hohe Zufriedenheit der Betroffenen oder ein grosses Unwissen über ihre Rechte und deren Geltendmachung schliessen. Daneben können jedoch auch weitere Faktoren wie die monetären und nichtmonetären Kosten, die Dauer und die Komplexität des Rechtsweges sowie Kosten-Nutzen-Überlegungen zu einer tiefen Anzahl Klagen beitragen.

Abbildung 2-2: Wirkungsmodell des schweizerischen Datenschutzgesetzes



Wirkungsmechanismus des EDÖB

Der zweite Wirkungsmechanismus baut auf das Prinzip der Intervention einer Behörde. Er legt die Verantwortung in die Hände des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Seine Kernaufgaben sind die Aufsicht über die Bearbeiter sowie die Beratung und die Information der Betroffenen und der Bearbeiter. Er trifft von sich aus oder auf Meldung von Dritten hin Abklärungen über die Rechtmässigkeit von Datenbearbeitungen, gibt aufgrund seiner Erkenntnisse Handlungsempfehlungen an Bearbeiter ab und setzt diese wenn nötig gerichtlich durch. Im Rahmen dieser Aufsichtstätigkeit versucht er direkt auf die Durchsetzung des Datenschutzrechts hinzuwirken. Der EDÖB handelt in diesen Fällen überwiegend *reaktiv*: Er wird in der Regel erst aufgrund von Hinweisen auf eine mutmassliche, bereits begangene Verletzung des DSG aktiv. Ergänzend dazu sind die Datenbearbeiter zur Meldung bestimmter Daten-

bearbeitungen an ihn verpflichtet (Register der Datensammlungen, Datenbekanntgaben ins Ausland, medizinische Forschung).

Weiter berät der EDÖB die Betroffenen und die Bearbeiter. Er informiert sie auf dem Wege der Öffentlichkeitsarbeit über seine Aktivitäten sowie seine datenschutzrechtlichen Einschätzungen, und er gibt Hinweise zum Selbstschutz und für eine korrekte Datenbearbeitung. Diese nicht verbindlichen Aktivitäten zielen stark in Richtung einer verstärkten Sensibilisierung und haben im Gegensatz zur Aufsichtstätigkeit einen eher *präventiven* Charakter. Insbesondere die Informationstätigkeit zielt darauf ab, Breitenwirkung über einen einzelnen Fall hinaus zu erzielen.

Insoweit also der EDÖB zur Sensibilisierung beiträgt, verstärkt er die Fähigkeit der Betroffenen, sich selbst zu schützen und für ihre Rechte einzustehen, und er verstärkt die Bereitschaft und Befähigung der Bearbeiter zu einem gesetzeskonformen Umgang mit den persönlichen Daten der Betroffenen.

Neben den Kernaufgaben der Beratung, Information und Aufsicht wirkt der EDÖB mit Stellungnahmen zu Gesetzgebungsvorhaben auf eine datenschutzkonforme Ausgestaltung der schweizerischen Rechtsordnung in allen Anwendungsbereichen ein. Darüber hinausgehend ist er angehalten, die Zusammenarbeit mit ausländischen und kantonalen Datenschutzbehörden zu pflegen.

Die Position des EDÖB bei Datenbearbeitungen von Bundesorganen und privaten Bearbeitern ist nicht identisch. So hat der EDÖB über die Datenbearbeitungen von Bundesorganen aufgrund des Legalitätsprinzips und seiner Kompetenzen im Rahmen der Rechtsetzung einen umfassenderen Überblick als über jene von Privaten. Abklärungen über Datenbearbeitungen sind im Übrigen bei Privaten nur im – allerdings sehr offen umschriebenen – Verdachtsfall möglich (vgl. Ziffer 12.3.1).

Kontext

Die Sensibilität der Betroffenen und der Datenbearbeiter ist abhängig vom Kontext, in dem sich diese Akteure bewegen. Der Fokus wird dabei auf vier Kontextfaktoren und deren Folgen gelegt: Die Entwicklung der Informationstechnologie kann als Motor für die Einführung neuer Datenbearbeitungen betrachtet werden. Damit hängt der Wandel der Wirtschaft zusammen, die neue Datenbearbeitungen auf dem Markt einführt. Die Verbreitung neuer Anwendungen wird aber auch von den politischen Rahmenbedingungen bestimmt. So stellte sich in der Sicherheitspolitik z.B. die Frage nach neuen Überwachungstechnologien. Diesen Kräften auf Seiten der Bearbeiter steht die Gesellschaft mit prinzipiell wandelbaren Wertmustern gegenüber. So dürften die Wertorientierungen und Einstellungen zu den Themen wie Kommunikation, Privatsphäre, Öffentlichkeit und Sicherheit sowie weiterer datenschutzrelevanter Gebiete mitbestimmen, welche Anwendungen neuer Technologien begrüsst und damit genutzt, und welche abgelehnt werden. So hat sich etwa der Informationsaustausch zwischen den Individuen begünstigt durch die neuen Informationstechnologien in den Jahren seit der Einführung des DSG enorm ausgeweitet.

Von den Kontextfaktoren können dreierlei Wirkungen ausgehen: Erstens kann erwartet werden, dass der Kontext die Sensibilität der Datenbearbeiter und der Betroffenen und damit deren Ver-

haltensweisen beeinflusst. Davon ausgehend wird zweitens vermutet, dass der Kontext die Erwartungen der Bearbeiter und der Betroffenen an das Gesetz beeinflusst. Drittens kann erwartet werden, dass die Wirksamkeit des Gesetzes von der Ausprägung des Kontexts abhängt.

2.3 Vorgehen der Evaluation

Die Vorgaben zur Evaluation des Datenschutzgesetzes machten einen interdisziplinären Ansatz erforderlich, der durch die Zusammensetzung des Evaluationsteams mit sozialwissenschaftlichem, juristischem und demoskopischem Fachwissen sichergestellt wurde. Entsprechend vielfältig sind auch die Methoden, die im Rahmen dieser Untersuchung zur Anwendung kamen. In diesem Kapitel wird das gewählte Vorgehen beschrieben.

Die Evaluation nimmt die im Wirkungsmodell des vorigen Abschnitts erarbeiteten Faktoren im Rahmen verschiedener Bausteine wieder auf. Dabei wurden die Forschungsarbeiten in drei Phasen gegliedert: Die erste Phase diente der Erhebung der Grundlagen und der Orientierung, zielte somit eher in die Breite. Die zweite Phase diente der thematisch fokussierten und vertieften Analyse der beiden Wirkungsmechanismen (Rechtsweg, EDÖB) sowie der Datenschutz-Sensibilität der Betroffenen. Die dritte Phase umfasste die Synthesearbeiten. Abbildung 2-3 gibt einen Überblick über die verschiedenen Bausteine und Phasen der Evaluation des DSG.

Die erste Phase umfasste folgende Bausteine:

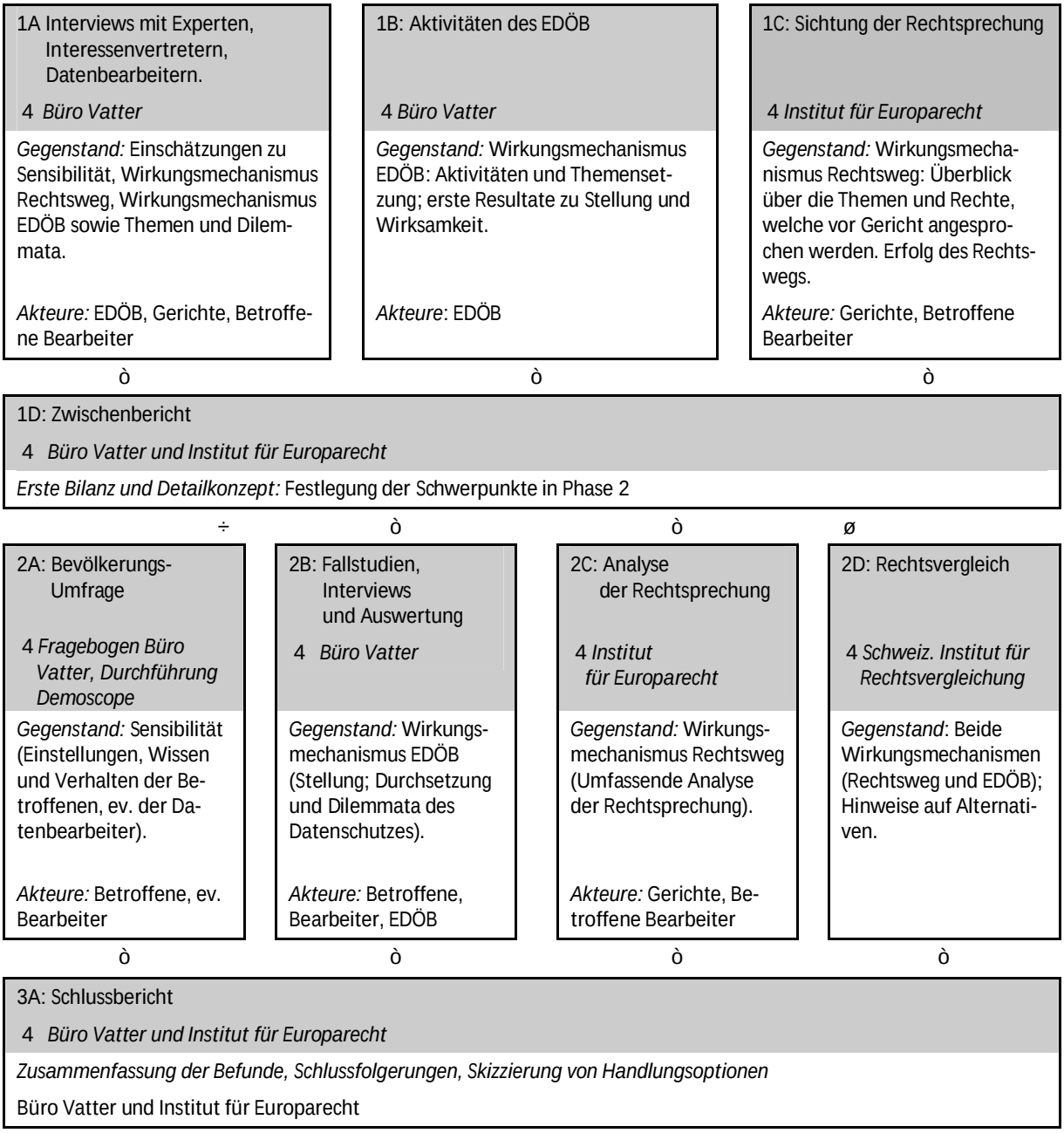
- *19 Leitfadeninterviews mit Rechts- und Technologieexperten, Interessenvertretern sowie privaten und öffentlichen Datenbearbeitern (Baustein 1A):* Einschätzungen zu aktuellen und künftigen Herausforderungen für den Datenschutz, zur Sensibilität der betroffenen Personen und der Datenbearbeiter sowie zu den beiden Wirkungsmechanismen waren Gegenstand der Interviews. Ergänzend wurde eine Literaturrecherche und Auswertung von parlamentarischen Vorstössen vorgenommen. Festzuhalten ist, dass bei den Interviews mit den Bearbeitern der Fokus in Absprache mit dem Auftraggeber stärker auf die Datenbearbeitung im Privatbereich gelegt wurde (vgl. auch Liste der Interviews in Anhang 1).[3]

- *Analyse der Aktivitäten des EDÖB (Baustein 1B):* Gruppeninterviews mit verschiedenen Mitarbeitenden des EDÖB zur Steuerung der Geschäfte und zu seinen Hauptaktivitäten, Sichtung und Auswertung bestehender Literatur und Auswertung bestehender Dokumente des EDÖB zu unterschiedlichen Aspekten des EDÖB (Aktivitäten, Stellung, Arbeitsabläufe).

- *Sichtung der Rechtsprechung (Baustein 1C):* Drittens erfolgte eine erste Auswertung der Rechtsprechung des Bundesgerichts und Bundesverwaltungsgerichts sowie der Rechtsprechung der Eidgenössischen Datenschutz- und Öffentlichkeitskommission (1993 bis 2006) und der kantonalen Behörden.

[3] Es bestehen bereits Untersuchungen mit Fokus auf den Bundesbereich: Bolliger/Féraud 2010 untersuchen den Datenaustausch zwischen Behörden; zwei Projekte befassen sich u.a. mit dem Zusammenspiel von Bundesorganen und dem EDÖB (GPK-N 2003; EFK 2007).

Abbildung 2-3: Bausteine und Phasen der Evaluation im Überblick



Basierend auf den Bausteinen 1A bis 1C erarbeitete das Evaluationsteam einen Zwischenbericht einschliesslich eines Detailkonzepts im Hinblick auf die zweite Phase. Dabei wurden die zentralen Stossrichtungen der Vertiefungsphase (Ausrichtung der Bevölkerungsbefragung, Auswahl der Fallstudien) gemeinsam mit der Arbeitsgruppe Evaluation DSG festgelegt. Die zweite Phase des Projekts wurde mit vier parallelen Forschungsstrategien angegangen: Im Zentrum standen die im Rahmen des Wirkungsmodells erarbeiteten Faktoren der *Datenschutz-Sensibilität* sowie die Wirksamkeit der beiden Durchsetzungsmechanismen *Rechtsweg* und *EDÖB*. Konkret umfasste die zweite Phase folgende Bausteine, die jeweils zu verschiedenen Teilen der Evaluation einen Beitrag zu leisten vermögen:

- *Bevölkerungsbefragung (Baustein 2A):* Mit der Bevölkerungsbefragung werden die verschiedenen Dimensionen der Sensibilität der betroffenen Personen erhoben: Allgemeine Einstellungen, datenschutzrelevantes Wissen sowie Selbstschutzmassnahmen und das Verhalten in konkreten datenschutzrelevanten Situationen (vgl. auch Fragebogen und technischen Bericht im Anhang 2 resp. 3).

- *Fallstudien (Baustein 2B):* Die Fallstudien behandeln hauptsächlich die Wirksamkeit des EDÖB in den Bereichen Aufsicht, Beratung und Information. Es wurden zehn Fallstudien erarbeitet. Sechs Fallstudien betreffen Bearbeitungen im Privatbereich, deren vier Bearbeitungen von Bundesorganen. Sie fussten auf einer Analyse der verfügbaren Dokumente des EDÖB und einer Recherche des Kontexts, auf zwei Gruppengesprächen mit Mitarbeiterinnen und Mitarbeitern des EDÖB und vier Befragungen von Datenbearbeitern (wovon je zwei private und zwei Bundesorgane). Darüber hinaus fand in der zweiten Phase ein weiteres Gespräch mit dem EDÖB statt.

- *Analyse der Rechtsprechung (Baustein 2C):* In diesem Baustein stand der erste beschriebene Wirkungsmechanismus des DSG im Zentrum: Die Rechtsprechung zum DSG sowohl auf kantonaler als auch auf nationaler Ebene wurde quantitativ (Häufigkeit der Inanspruchnahme und Erfolg) und qualitativ (Auslegung des Gesetzes durch die Gerichte) ausgewertet.

- *Rechtsvergleich (Baustein 2D):* Der Rechtsvergleich wurde parallel zu den Arbeiten an dieser Evaluation vom Schweizerischen Institut für Rechtsvergleichung erarbeitet (SIR 2010). Er dient insbesondere dazu, das schweizerische Gesetz im internationalen Vergleich darzustellen sowie Inputs für Verbesserungsmöglichkeiten beider Wirkungsmechanismen und des Gesetzes im Allgemeinen zu gewinnen. Berücksichtigt wurden dabei folgende Länder (alphabetisch geordnet): Deutschland, Frankreich, Italien, Kanada, Niederlande, Österreich, Schweden, Slowenien und Spanien. Im Zusammenhang mit Regelungen, welche sich auf neue Informations- und Kommunikationstechnologien beziehen, wurden zusätzlich Regelungen aus Gliedstaaten der USA berücksichtigt.

Im Rahmen der dritten Projektphase wurden die Erträge aus den Bausteinen 1A bis 2D zusammengeführt. Abschliessend wurden Schlussfolgerungen gezogen sowie mögliche Handlungsoptionen hergeleitet (Teil V des vorliegenden Berichts).

TEIL II: TECHNOLOGISCHE, WIRTSCHAFTLICHE UND GESELLSCHAFTLICHE RAHMENBEDINGUNGEN

Dieser Teil der Evaluation widmet sich schwerpunktmässig der Sensibilität der beiden Akteursgruppen, die im Zentrum des Wirkungsmodells (vgl. Kapitel 2) stehen: den privaten und staatlichen Datenbearbeitern auf der einen sowie den betroffenen Personen auf der anderen Seite. Die Ausprägung der Sensibilität in diesen zwei Gruppen hat Auswirkungen auf die Wirksamkeit der Durchsetzungsmechanismen des Datenschutzgesetzes, die Gegenstand der anschliessenden Teile III und IV sein werden. Vorangestellt wird die Frage, welche neuen technologischen Entwicklungen den Datenschutz vor besondere Herausforderungen stellen. Auch wird nach den Konsequenzen dieses Wandels für das Datenschutzgesetz und dessen Umsetzung gefragt.

Dieser Teil ist folgendermassen aufgebaut: Kapitel 3 befasst sich mit den technologischen Herausforderungen des Datenschutzes. Daran anschliessend wird der Frage nachgegangen, wie die Beachtung des Datenschutzes durch private Unternehmen und Bundesbehörden beurteilt werden kann (Kapitel 4). Schliesslich wird in Kapitel 5 vertieft die Sensibilität der Bevölkerung thematisiert. Neben der Erfassung von Einstellungen zur Bedeutung des Datenschutzes und des Informationsaustauschs für die Betroffenen werden spezifisch auch die Anwendung von Massnahmen zum Selbstschutz, das Verhalten in konkreten, datenschutzrelevanten Entscheidungssituationen (Umgang mit persönlichen Angaben in Sozialen Netzwerken oder beim Kauf einer Dienstleistung, Massnahmen der Datensicherheit) sowie Kenntnisse über bestimmte Datenbearbeitungen thematisiert. Am Ende dieses Teils werden die Befunde zusammengefasst und eine Bilanz gezogen.

3 Technologische Herausforderungen für den Datenschutz

In diesem Kapitel soll eine Auslegeordnung der technologischen Herausforderungen, die sich dem Datenschutz stellen, vorgenommen werden. Im Weiteren werden technische Möglichkeiten, die den Schutz von Personendaten unterstützen können, sowie mögliche Auswirkungen auf den Datenschutz als Folge dieser Entwicklungen diskutiert. Die Ausführungen stützen sich überwiegend auf Interviewaussagen der Technologie- und Rechtsexperten, ergänzt um Einschätzungen des EDÖB und der Interessenvertreter sowie auf Literaturbeiträge.

3.1 Allgemeine technologische Herausforderungen

Die technologischen Herausforderungen werden nachfolgend anhand von vier Aspekten beschrieben: zunehmende Leistungsfähigkeit und Speicherkapazität von Computern und Netzwerken, zunehmende Miniaturisierung und Digitalisierung, Mengenausweitung persönlicher Daten und verbesserte Auswertungsmöglichkeiten.

3.1.1 Zunehmende Leistungsfähigkeit und Speicherkapazitäten

Die interviewten Technologieexperten verwiesen in ihren Aussagen weniger auf spezifische Anwendungen, sondern machten in erster Linie auf generelle Trends aufmerksam: So nehmen die Leistungsfähigkeit von Computern und die Übertragungskapazität der Netze ständig zu. Dieses Wachstum bewirke, dass Datenbearbeiter kaum noch technische Restriktionen zu beachten haben. Informationen können somit umfangreich erhoben, gespeichert, kopiert und während langer Zeit aufbewahrt werden. Datenbearbeitungen, die vor Jahren noch Tage oder Stunden in Anspruch genommen haben, können heute innert kürzester Zeit durchgeführt werden. Die befragten Technologieexperten gehen davon aus, dass sich diese Entwicklung auch in Zukunft fortsetzen wird. Gemäss dem Mooreschen Gesetz komme es alle 18 Monate zu einer Verdoppelung der Leistungsfähigkeit von Computern und Netzwerken.

3.1.2 Zunehmende Miniaturisierung und Digitalisierung

Die technologische Entwicklung hat dazu geführt, dass technische Geräte heute fast beliebig klein sind und drahtlos funktionieren können. Eine Folge davon ist, dass es heute permanent und überall möglich ist, aufs Internet zuzugreifen, z.B. via Mobiltelefon. Daneben existieren eine Reihe weiterer Gegenstände, die Daten erheben und zum Teil selbständig mit dem Internet kommunizieren können (z.B. Videokameras, RFID-Chips). Immer mehr Lebensbereiche werden von dieser Digitalisierung erfasst (Stichwort „allgegenwärtige Datenbearbeitungen“): Experten erwarten, dass in der Zukunft die Tendenz zum „Internet der Dinge“ (vgl. z.B. Mattern 2003; Mattern/Floerkemeier 2010) fortschreiten wird. Darunter versteht man die elektronische Vernetzung von Gegenständen im Alltag und deren selbständige Kommunikation untereinander. Es sind Services wie z.B. Brillen vorstellbar, die beim zufälligen Treffen eines Bekannten dessen Namen einblenden (Langheinrich/Mattern 2002).

3.1.3 Zunehmende Mengen persönlicher Daten

Diese Omnipräsenz führt dazu, dass die elektronischen Spuren, die von den Benutzern hinterlassen werden, immer mehr zunehmen. Für den Einzelnen ist es allein schon aufgrund der Menge an Daten viel schwieriger geworden, die Übersicht über die persönlichen Daten zu erhalten und eine gewisse Kontrolle über ihre Verwendung durch andere auszuüben. Gleichzeitig können diese Spuren immer besser aufgezeichnet werden (z.B. Tracking im Internet, aber auch in der realen Welt via GPS-Chip im Mobiltelefon). Die befragten Experten gehen davon aus, dass auch dieser Trend sich in Zukunft weiter verstärken werde. Als weiteren wichtigen Punkt erwähnten die Interviewpartner, dass die Zahl der Nutzerinnen und Nutzer des Internets und verschiedenerer weiterer Anwendung stark zugenommen habe.

Die genannten technologischen Entwicklungen und neuen Möglichkeiten sowie deren immer intensivere Nutzung durch einen stetig wachsenden Personenkreis führen somit dazu, dass Nutzerinnen und Nutzer immer mehr Spuren über ihr Verhalten und somit Personendaten hinterlassen, die gespeichert und bearbeitet werden können. Diese Spuren entstehen in der physischen, aber auch in der virtuellen Welt, wobei die Grenzen zwischen diesen Welten zunehmend verschwinden. Die meisten gesammelten Daten werden heute digital gespeichert, und die Speichermedien sind zunehmend vernetzt, auch über Landesgrenzen hinweg: Die Datenbearbeitungen beschränken sich im virtuellen Raum nicht mehr auf die Schweiz, sondern häufig sind auch ausländische Akteure involviert.

3.1.4 Verbesserte Auswertungsmethoden

Die gesammelten Informationen können immer besser ausgewertet werden, denn auch die technischen Möglichkeiten, mit denen grosse Datenbestände analysiert und Datensätze miteinander verknüpft werden können, werden immer ausgefeilter (Stichwort „Data Mining“). Damit können aus unterschiedlichen Datensätzen Informationen gewonnen werden, die sich aus den einzelnen, isolierten Daten nicht ergeben. Die interviewten Experten weisen darauf hin, dass die Algorithmen zur Auswertung von Informationen mittlerweile auch Bilder, Videos und Audiodateien umfassen können. Es besteht somit die Möglichkeit, unterschiedlichste, im Einzelnen womöglich wenig sensible Informationen zueinander in Beziehung zu stellen und dadurch aussagekräftige Persönlichkeitsprofile zu erstellen.

Von diesen verbesserten Analysemöglichkeiten geht zudem der Effekt aus, dass es für Datenbearbeiter Sinn macht, möglichst viele Daten zu sammeln: Einerseits stellt der Speicherplatz keine Restriktion mehr dar; andererseits können Informationen, die heute noch nicht sinnvoll bearbeitet werden können, in Zukunft für die Bearbeiter von grossem Nutzen sein.

3.2 Spezifische Anwendungen

Die interviewten Technologieexperten richteten in ihren Aussagen den Fokus betont auf die genannten übergeordneten Entwicklungen und weniger auf spezifische, einzelne Applikationen. Trotzdem wurden einige konkretere Entwicklungen, Anwendungen oder Technologien genannt,

die aus einer datenschutzrechtlichen Sicht als heikel eingestuft werden. Die folgende illustrative Zusammenstellung gibt dabei insbesondere die Einschätzungen der Technologieexperten wider und ist somit nicht als abschliessende Auflistung zu verstehen.[4]

- *Massgeschneiderte Werbung im Internet:* Mit Hilfe von Cookies[5] wird registriert, mit welchen Angaben sich jemand für eine Website anmeldet, und es werden Merkmale wie Alter, Einkommen, aber auch das Einkaufsverhalten eines Internetnutzers geschätzt, indem sein Surfverhalten in Echtzeit verfolgt wird (sog. Tracking). Mithilfe von Algorithmen lassen sich aus den gesammelten Daten über die aufgerufenen Internetseiten Benutzerprofile bilden. Damit haben Unternehmen z.B. die Möglichkeit, ihren Werbeauftritt auf diese Profile abzustimmen.

- *Soziale Netzwerke im Internet:* Soziale Netzwerke unterscheiden sich insbesondere dadurch von anderen „klassischen" Datenschutzproblemen, dass die Benutzer selber ihre Informationen zur Verfügung stellen, und dass in besonders hohem Masse auch Dritte (z.B. durch die Veröffentlichung von Fotos) betroffen sein können. Als Problem wird darüber hinaus erachtet, dass den Nutzerinnen und Nutzern oft nicht bewusst sei, welchem Kreis von Personen sie ihre Angaben eigentlich zur Verfügung stellen und sie den entsprechenden Steuerungsmöglichkeiten, die durchaus vorhanden sind, deshalb zu wenig Beachtung schenken.

- *Cloud Computing:* Cloud Computing meint, dass Dokumente, Internetseiten, Fotos oder Videos nicht auf einem eigenen Rechner gespeichert werden, sondern „in der Wolke", womit über die ganze Welt verteilte Datenzentren gemeint sind. Die Nutzerinnen und Nutzer können von überall und mit verschiedenen Geräten auf ihre Daten zugreifen und mit anderen Nutzern teilen. Aus Sicht des Datenschutzes stellen sich vor allem Fragen der Datensicherheit und der Vertrauenswürdigkeit der Anbieter solcher Dienstleistungen.

- *Online-Dienstleistungen im Allgemeinen:* Immer häufiger werden im Internet Dienstleistungen erbracht und dabei Personendaten bearbeitet. Beispiele sind: Einkäufe, Unfallmeldungen, Wettbewerbsteilnahmen, Online-Banking. Als störend wird seitens der Technologieexperten vor allem die Tatsache beurteilt, dass häufig eine Reihe von Angaben zur Person gemacht werden müsse, um die Dienstleistungen in Anspruch nehmen zu können.

- *Lokalisierung:* Zu einer zunehmend wichtigen Gruppe von Anwendungen zählen die Technologieexperten Techniken, mit denen der Aufenthaltsort von Personen bestimmt resp. Personen identifiziert werden können (z.B. GPS-Systeme oder RFID-Chips). Damit ist es möglich, Personen zu lokalisieren und zu überwachen.

- *Videoüberwachung:* Die Videoüberwachung schliesslich ist von den Technologieexperten nicht spezifisch erwähnt worden. Andere Interviewpartner dagegen sehen in diesem Bereich grosse Herausforderungen und bedeutsamen Regelungsbedarf.

4 Für eine Aufzählung weiterer neuer technologischer Herausforderungen vgl. etwa Thür (2010).
5 Vom Datenbearbeiter auf dem Computer des Nutzers installierte Kleinprogramme.

3.3 Datenschutzfreundliche Technologien

Die Technologieexperten wurden ebenfalls befragt, inwiefern die Technologie selber zur Sicherung des Datenschutzes unter den heutigen Bedingungen beitragen könne. Hier zeigte sich, dass grundsätzlich eine Reihe von „datenschutzfreundlichen" Technologien vorhanden wäre, die den Schutz von Personendaten unterstützen könnten. Als Beispiele dafür wurden genannt: Anonymisierung; Verschlüsselung (auch von Bilddaten); Klassifizierung von Dokumenten; Erstellung unterschiedlicher Zugriffsberechtigungen (z.B. Pin, Smart Card); P3P-Profile.

Daneben wurde in den Interviews auf die Möglichkeit verwiesen, einzelne Daten mit „Klauseln" zu versehen, welche darüber Auskunft geben, wie die Daten vom Bearbeiter verwendet werden können. Solche Klauseln können beispielsweise den Bearbeitungszweck oder eine Löschfrist beinhalten. Ein Potenzial wird zudem in der Regionalisierung oder Lokalisierung der Datenbearbeitung gesehen. Technisch sei es heute möglich, Daten geografisch zu binden und so die möglichen Datenbearbeitungen auf ein bestimmbares Gebiet zu beschränken.

Allerdings stehen der Anwendung dieser Möglichkeiten in der Praxis gewisse Hürden im Weg. So wird insbesondere darauf verwiesen, dass die Benutzerfreundlichkeit solcher Technologien zum Teil noch nicht sehr hoch sei; gerade für kleinere und mittlere Firmen wäre eine benutzerfreundliche Anwendbarkeit von grosser Bedeutung. Ebenfalls wurde seitens der Technologieexperten argumentiert, dass für die Bearbeiter kaum Anreize bestünden, Investitionen in datenschutzfreundliche Technologien zu tätigen. Der Grund wird darin gesehen, dass den Ausgaben und dem Aufwand in diesem Fall kaum ein Nutzen gegenüberstehen dürfte: Die quantifizierbaren Kosten einer Datenschutzverletzung werden als zu gering erachtet, als dass sich eine Einführung derartiger Methoden für ein Unternehmen lohnen würde.

3.4 Folgen für den Datenschutz

Die technologische Entwicklung und die Verbreitung der neuen Anwendungen stellen den Datenschutz vor Herausforderungen. In diesem Abschnitt sollen deshalb spezifische Auswirkungen diskutiert werden. Dabei wird nach den Folgen für die betroffenen Personen sowie für die Technologieneutralität und die Grundsätze des DSG gefragt; schliesslich werden mögliche Auswirkungen auf die beiden Wirkungsmechanismen des schweizerischen Datenschutzgesetzes thematisiert

3.4.1 Herausgeforderte Betroffene

Die neuen technischen Möglichkeiten und Anwendungen haben dazu geführt, dass die Menge an persönlichen Daten, welche Individuen über sich generieren und hinterlassen, enorm zugenommen hat. Bei der Entstehung dieser Spuren hat der Betroffene sehr unterschiedliche Kontroll- und Einflussmöglichkeiten. Es lassen sich diesbezüglich drei Entstehungsarten von Spuren unterscheiden:

- *Aktive Preisgabe von Daten:* Spuren resultieren erstens aus bewussten und mehr oder minder freiwillig gemachten Angaben zuhanden von Dritten. Beispiele dafür sind Antworten auf ei-

ne Umfrage, das Ausfüllen Formulars einer Behörde oder beim Bestellen einer Leistung, das Einreichen eines Bewerbungsdossiers für eine Stelle, das Diskutieren in einem Chatroom im Internet oder das Hochladen von Informationen in einem Sozialen Netzwerk. Hier kann von einer vergleichsweise hohen Kontrollmöglichkeit der Betroffenen ausgegangen werden (solange sie nur Informationen über sich selbst preisgeben). Abgesehen von obligatorisch vorgesehenen Datenbekanntgaben ist es weitgehend ihrer Eigenverantwortung überlassen, wem sie welche Angaben machen..

- *Passives hinterlassen von Spuren:* Für Dritte zugängliche Spuren entstehen zweitens, ohne dass sich die betroffene Person aktiv äussert, bewusst ihr Einverständnis dazu gibt oder überhaupt etwas davon merkt. Typisch hierfür sind die Möglichkeiten zur Lokalisierung in der realen Welt (z.B. über einen GPS-Chip im Mobiltelefon), aber auch Bewegungsdaten aus der virtuellen Welt, indem aufgezeichnet wird, welche Internetadressen eine Person besucht hat. Gerade auch hinsichtlich des Internets der Dinge erhält die unaufdringliche und im Hintergrund ablaufende Erhebung und Bearbeitung von Daten eine zunehmende Bedeutung (Mattern/Floerkemeier 2010). Teilweise kann über die Einstellung der Geräte und Anwendungen die Menge der hinterlassenen oder erkennbaren Daten gesteuert werden. Wird diese Gelegenheit nicht wahrgenommen, etwa, weil sie dem Betroffenen nicht bekannt ist oder mit einer Einschränkung einer Anwendung verbunden ist, ist seine Kontrolle tief.

- *Beschaffung von Daten wider den Willen des Betroffenen:* Zugänglich sind Spuren drittens auch gegen den aktiven Willen der Personen, weil sich Dritte widerrechtlich Zugang dazu verschaffen, oder weil die legitimen Empfänger der Daten diese entgegen anders lautenden Vereinbarungen aufbewahren, weitergeben, veröffentlichen oder nur unzureichend schützen. Das Hacking von Computern oder die Speicherung von Ortungsdaten von Mobiltelefonen wider anders lautender Versprechen des Anbieters sind Beispiele hierfür. Auch hier sind Sicherheitsvorkehrungen möglich (Firewall, Cookie-Filter, etc. im Internet), aber grundsätzlich sind die Schutzmöglichkeiten begrenzt. Der Datendiebstahl im Einzelfall erfolgt unbegrenzt.

Unabhängig vom Grad der Selbstschutzmöglichkeiten bei der Bekanntgabe, müssen die Betroffenen prinzipiell davon ausgehen, dass einmal bekannt gegebene Daten heute mit viel grösserer Wahrscheinlichkeit weitergegeben und für andere Zwecke weiterverwendet werden können, als ursprünglich beabsichtigt war. Das Berichtigungsrecht und das Recht auf Vergessen sind im Zeitalter des Internets gemäss den Aussagen der Interviewpartner kaum noch aufrechtzuerhalten. Die Verbreitung neuer Technologien und Anwendungen hat nach Aussagen der befragten Personen insbesondere in den jüngeren Altersgruppen zu einem gewissen Druck geführt, diese auch zu nutzen. Dies gelte insbesondere im Bereich der Mobilkommunikation und des Internets und hier vor allem für die Sozialen Netzwerke.

Diese Entwicklungen stellen für die betroffenen Personen Herausforderungen dar: Sie stellen hohe Anforderungen an die Kompetenz im Umgang mit neuen technischen Anwendungen und Geräten sowie an die Eigenverantwortung der Nutzerinnen und Nutzer. Gleichzeitig sind die Interviewpartner der Meinung, dass es heute für den Einzelnen nicht mehr möglich sei zu wissen, wo überall persönliche Daten abgespeichert sind und wer diese Daten wozu bearbeitet. Ein

Technologieexperte geht davon aus, dass alles, was im Internet veröffentlicht worden ist, als allgemein bekannt betrachtet werden muss.

3.4.2 Technologieneutralität des DSG und internationaler Vergleich

Das DSG ist technologieneutral formuliert. Das heisst, es gilt unabhängig der verwendeten Technologien und enthält keine Spezialbestimmungen hinsichtlich bestimmter Anwendungen. Die befragten Interviewpartner sind mehrheitlich der Meinung, dass an diesem Prinzip nichts geändert werden sollte; auch die Mitarbeiter des EDÖB vertraten im Interview diese Ansicht. Dennoch ist es sinnvoll, angesichts der rasanten Entwicklungen und im Rahmen der rechtsvergleichenden Analyse (SIR 2010) auf die Frage einzugehen, wie das Verhältnis von Technologie und Datenschutzgesetzgebung ausgestaltet ist. Dabei werden zusätzlich zwei Gliedstaaten der USA (Massachusetts und Kalifornien) berücksichtigt, welche diesbezüglich spezielle Ansätze verfolgen.

Im europäischen Gemeinschaftsrecht bestehen Sonderreglungen für automatisierte Einzelentscheidungen (Art. 15 Richtlinie 95/46/EG) sowie zur elektronischen Kommunikation (Richtlinie 2002/58/EG). Nach der Richtlinie 2002/58/EG müssen Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Massnahmen ergreifen, um die Sicherheit seiner Dienste (inkl. Netzsicherheit) zu gewährleisten. Daneben bestehen restriktive Vorschriften zur Verarbeitung von Verkehrsdaten und deren Speicherung (Verarbeitung und Speicherung nur zur Gebührenabrechnung), sowie weitere detaillierte Vorschriften. Dabei geht es darum, die jeweiligen Operationen nur mit Zustimmung zu erlauben („Opt-in-Prinzip“) oder mindestens ein „opting out” zu ermöglichen. Die Umsetzung dieser Vorschriften erfolgte in verschiedenen Staaten im Datenschutzrecht (insbesondere in den UK und in Italien), in anderen Staaten in Spezialgesetzen (z.B. Deutschland, Österreich, Frankreich).

Teilweise finden sich spezifischere Regelungen in bestimmten Bereichen. Im Rahmen der Datenschutzgesetze finden sich z.B. ausdrückliche Regeln zur Biometrie, zum Direktmarketing (Slowenien) oder zur Verwendung mobiler personenbezogener Speicher- und Verarbeitungsmedien (Deutschland). Im Weiteren enthalten das deutsche, österreichische und slowenische Recht Vorschriften hinsichtlich der Videoüberwachung.

In Massachusetts wurde kürzlich ein neues Gesetz erlassen, welches für Datenbearbeitungen ein regelrechtes Informationssicherungsprogramm verlangt. Dabei muss ein risikoorientierter Ansatz verfolgt werden. Es bestehen besondere Vorschriften zum Schutz von Computernetzwerken und eine weitgehende Verpflichtung zur Verschlüsselung von elektronisch übermittelten und gespeicherten Informationen. Das Prinzip von „Privacy by Design“ wird damit zur allgemeinen Pflicht.

In Kalifornien findet sich kein allgemeines Datenschutzgesetz, doch Regeln zu neuen Technologien finden sich einer Vielzahl von Gesetzen. Besondere Aufmerksamkeit widmet der Gesetzgeber dabei der Problematik des „Identity Theft“, d.h. der Verwendung einer anderen Identität zu Täuschungszwecken. Neben Strafbestimmungen und Strafverfolgungsmassnahmen (u.a. spezialisierte Strafverfolgungseinheiten) ermöglicht die Gesetzgebung den Betroffenen besondere Korrekturmechanismen. Ein anderer Bereich, in welchem eine Vielzahl von Bestimmungen bestehen,

ist das Sammeln von Daten mit elektronischen Hilfsmitteln. Dabei wird das Sammeln teils sektorspezifisch (z.B. in der Automobilindustrie), teils eher allgemein (Aufnahmen in Privatsphäre) geregelt. Auch im Informatikbereich und in der Telekommunikation besteht eine Vielzahl sehr spezifischer Vorschriften: Als neuste gesetzgeberische Initiative ist die momentan debattierte Regulierung von Sozialen Netzwerken zu erwähnen; dabei soll den Betreibern die Veröffentlichung der Adresse und Telefonnummer von Benutzern unter 18 Jahren verboten werden (SIR 2010: 280). Trotz dieser Vielzahl gesetzlicher Grundlagen beeinflussen durchwegs ähnliche Grundsätze die Regelungen: Das Sammeln und Speichern von Daten ist nur für bestimmte Zwecke oder/und mit dem Einverständnis der betroffenen Person zulässig, was darüber hinaus geht, ist verboten. Oft haben die Betreiber oder die Sammler besondere Hinweispflichten. Schliesslich findet sich vielerorts eine Schadenersatzpflicht.

3.4.3 Folgen für die Grundsätze des DSG, insbesondere die Zweckbindung

Die beschriebenen Entwicklungen im Technologiebereich tangieren die Grundsätze des DSG. Spezifisch wurde in den Interviews der Grundsatz der Zweckbindung behandelt: Dieser sei aufgrund der technologischen Entwicklungen immer schwieriger durchzusetzen. Als problematisch erweise sich insbesondere das Data Mining, bei dem grosse Datenmengen ausgewertet und dadurch neue Erkenntnisse über Personen gewonnen werden, die nicht mehr dem Zweck der ursprünglich erhobenen Daten entsprechen. Die Zweckbindung einer Datenbearbeitung ist nach der Weitergabe durch den Dateninhaber an Dritte vom Empfänger der Daten einzuhalten (Maurer-Lambrou/Vogt 2006: 83; Rosenthal/Jöhri 2009: 95): Somit dürfte auch deshalb die Zweckbindung immer schwieriger einzuhalten sein, da Daten rasch kopiert und weiterverbreitet werden können (auch ohne das Wissen des Inhabers einer Datensammlung).

Zudem wurde darauf hingewiesen, dass es Firmen gebe, die Daten auf Vorrat sammeln, ohne zum Zeitpunkt der Datenerhebung bereits zu wissen, wozu die Daten verwendet werden. Die Unternehmen gingen in diesen Fällen davon aus, dass die auf Vorrat gesammelten Daten in Zukunft mit moderneren Auswertungsverfahren bearbeiten und nützliche Informationen gewinnen können.

Im Rahmen der Interviews wurde verschiedentlich auf eine mangelnde Sensibilität der Betroffenen hingewiesen. Erwähnt wurden in diesem Zusammenhang, dass die Betroffenen häufig den Grundsatz der Zweckbindung einer Datenbearbeitung gar nicht kennen würden, sowie die fehlende Aufmerksamkeit bei der Preisgabe von persönlichen Informationen, z.B. beim Durchlesen der Allgemeinen Geschäftsbedingungen. Ein Rechtsexperte machte darauf aufmerksam, dass es für Firmen mitunter eine vergleichsweise risikoarme Strategie sei, relativ offen darüber zu informieren, was mit den Daten gemacht werde, weil die Wahrscheinlichkeit, dass von Seiten der Betroffenen Widerstand komme, sehr klein sei. Auch sei es möglich, durch eine relativ offene Formulierung des Verwendungszweckes den Grundsatz der Zweckbindung teilweise zu umgehen.

Trotz der erschwerten Durchsetzbarkeit der Zweckbindung beurteilen die befragten Rechtsexperten und Interessenvertreter den Grundsatz als richtig und wichtig. Es wurde argumentiert, dass die Zweckbindung nicht einfach mit der Begründung aufgehoben werden könne, dass sie unter den heutigen Gegebenheiten nicht mehr in allen Fällen umgesetzt werde. Ein Technologie-

experte beurteilt die Zweckbindung in der heutigen Zeit als überholt. Er begründet diese Aussage damit, dass heute Personen Daten häufig von sich aus zur Verfügung stellen. Die beiden befragten Rechtsexperten sehen die Zweckbindung als denjenigen Grundsatz des DSG, der am schwierigsten aufrechtzuerhalten ist. Dennoch haben die geschilderten Entwicklungen auch Folgen auf die Grundsätze von Treu und Glauben sowie der Erkennbarkeit. Insgesamt bestand in den Interviews Einigkeit darüber, dass die Grundsätze des DSG nach wie vor richtig sind.

3.4.4 Herausforderung für die Wirkungsmechanismen des DSG

Abschliessend soll gefragt werden, wie die Wirkungsmechanismen des DSG unter den veränderten Rahmenbedingungen zu beurteilen sind. Nach Rossnagel (2007: 85f.) greift das Schutzkonzept des Datenschutzrechts vor dem Hintergrund des technologischen Wandels nicht in allen Fällen ins Leere. Auch für neue Anwendungen lasse sich die rechtliche Erlaubnis einer Datenbearbeitung überprüfen und datenschutzrechtliche Grundsätze zur Anwendung bringen. Allerdings knüpft er diese Feststellung an gewisse Bedingungen, die erfüllt sein müssen: klare und einfache Frontstellung zwischen Datenbearbeiter und Betroffenen; Prozesse, deren Wirkungen einzelnen Verantwortlichen zuzurechnen sind; die zu beurteilenden Handlungen betreffen Einzelfälle.

Angesichts der neuen technologischen Entwicklungen verändern sich die Interaktionen zwischen Menschen jedoch grundsätzlich: Die Zahl der Beteiligten mit ständig wechselnden Rollen nimmt zu, vielfältige Zwecke werden gleichzeitig verfolgt, Daten werden in verschiedenen Kontexten (privat/geschäftlich) verwendet, die Datenbearbeitung erfolgt zum Teil spontan von Techniksystemen selbst und für den Betroffenen unbemerkt; auch können die Datenbearbeitungen nicht ohne Weiteres einem bestimmten Akteur zugeordnet werden (fehlende Transparenz). Zudem sind die Wirkungen undurchschaubar. Die von Rossnagel aufgestellten drei Bedingungen sind somit immer häufiger nicht erfüllt, und die Grundsätze des Datenschutzes werden in Frage gestellt. Rossnagel fordert ein „modifiziertes und ergänztes Schutzprogramm“ (Rossnagel 2007: 90), in dem der Datenschutz der Allgegenwärtigkeit der Datenverarbeitung angepasst wird.

In Bezug auf das schweizerische Datenschutzgesetz ergibt sich die Frage, inwieweit die beschriebenen Entwicklungen die Wirksamkeit der bestehenden Wirkungsmechanismen aushebeln und inwieweit diese Mechanismen, welche die Einhaltung der Grundsätze des Datenschutzes sicherstellen sollen, weiterhin greifen. Zu vermuten ist, dass die Wirkungsmechanismen des DSG insbesondere dann nicht mehr ausreichend sind, wenn Datenbearbeitungen unbemerkt vollzogen werden, wenn nicht klar ersichtlich ist, wer überhaupt die Datenbearbeitungen durchführt, und wenn Datenbearbeitungen nicht in der Schweiz, sondern im Ausland durchgeführt werden.

In dieser Situation können uninformierte Betroffene ihre Rechte nicht geltend machen; informierte Betroffene und auch der EDÖB können nicht auf fehlbare Bearbeiter zugreifen, weil sie diese nicht identifizieren können oder sie sich dem rechtlichen Zugriff entziehen.

Festzuhalten ist, dass die mit der technologischen Entwicklung entstandenen Datenbearbeitungen, die aus Sicht der Betroffenen durch unklare Verantwortlichkeiten und Verwendungszwecke gekennzeichnet sind, die konventionellen Bearbeitungen mit klarer Konstellation nicht abgelöst haben, sondern hinzugetreten sind. Nicht alle Datenbearbeitungen, die auf digitaler Datenverar-

beitung beruhen oder sich das Internet zunutze machen, sind somit aus Sicht der Betroffenen unübersichtlich. Aber auch die Anzahl Bearbeitungen in diesen eher klassischen Konstellationen mit klarer Verantwortlichkeit des Datenbearbeiters hat zugenommen.

4 Datenschutz bei privaten Bearbeitern und Bundesorganen

Dieses Kapitel beschäftigt sich mit den Akteuren, welche das DSG als Bearbeiter von Personendaten auffasst, den privaten Datenbearbeitern[6] und den Bundesorganen. Das Wirkungsmodell (vgl. Kapitel 2) beschreibt, welche Bedeutung von der Sensibilität der Datenbearbeiter ausgeht: Sind sie hoch sensibilisiert, wird ein hohes Datenschutzniveau erreicht, unabhängig davon, wie stark sich die Betroffenen für den Datenschutz einsetzen. Bei einer niedrigen Sensibilität muss dagegen von einem geringen Datenschutzniveau ausgegangen werden; in diesem Fall erhält die Sensibilität der Betroffenen eine hohe Bedeutung für die Durchsetzung des Gesetzes.

Im Mittelpunkt dieses Kapitels steht neben der konkreten Umsetzung des DSG und der Ausbildungsmöglichkeiten vor allem die Frage, mit welchen unternehmerischen und öffentlichen Zielsetzungen der Datenschutz kollidiert, und welche Risiken Firmen und Bundesorgane zur Einhaltung der rechtlichen Vorgaben veranlassen können. Vorgängig wird der Frage nachgegangen, in welchen Bereichen künftig besondere Herausforderungen für den Datenschutz entstehen.

Die Datengrundlage für dieses Kapitel bilden die Interviews mit Experten, Interessenvertretern, den Mitarbeitenden beim EDÖB sowie privaten Datenbearbeitern und Bundesorganen. Im Rahmen dieser Studie wurden Interviews mit Vertretern von acht privaten Datenbearbeitern und drei Bundesorganen durchgeführt. Dabei handelte es sich durchwegs um die in ihrem Betrieb, Departement oder Amt zuständigen Personen für den Datenschutz. Bei der Auswahl im Privatbereich wurde einerseits darauf geachtet, dass verschiedene Branchen, in denen Datenbearbeitungen eine wichtige Rolle spielen, berücksichtigt wurden; von den befragten Unternehmen sind deren sieben Mitglied im Verein Unternehmensdatenschutz (VUD). Es kann somit davon ausgegangen werden, dass die Sensibilität seitens der Interviewpartner hoch war, so dass der Verallgemeinerbarkeit der Ergebnisse Grenzen gesetzt sind.[7] Zudem werden bereits in diesem Kapitel einige Ergebnisse aus den Fallstudien berücksichtigt (vgl. dazu die Einleitung zu Teil IV).

4.1 Datenschutzrechtliche Herausforderungen

Einleitend werden wird zunächst diskutiert, welche Herausforderungen aufgrund der technologischen Entwicklungen (vgl. Kapitel 3) für den Datenschutz entstehen. Danach wird auf spezifische Herausforderungen in unterschiedlichen Themenbereichen eingegangen werden.

6 Wir beschränken uns in diesem Kapitel auf private Unternehmen. Gemeinnützige Organisationen oder natürliche Personen werden ausgeblendet.

7 Dies ist ein Nachteil der Auswahl der Interviewpartner. Der Vorteil, der diesen Nachteil überwiegt, ist, dass die befragten Personen allesamt über einschlägige Erfahrungen mit den DSG verfügen und so eine differenzierte Sicht auf das Gesetz ermöglicht wird.

4.1.1 Folgen der technologischen Entwicklungen für Datenbearbeiter

Private Datenbearbeiter

Verschiedentlich ist in den Interviews mit Technologie- und Rechtsexperten auf die ökonomische Dimension von Datenbearbeitungen hingewiesen worden. Persönliche Informationen haben für die Datenbearbeiter einen finanziellen Wert („Data is the new currency"). Insofern macht es aus Sicht von Unternehmen, die Daten bearbeiten, zum Teil Sinn, möglichst viele Informationen zu generieren und auszuwerten. So ist es beispielsweise für die gezielte Verteilung von Werbung ein Vorteil, wenn man die Adressaten hinsichtlich verschiedener Dimensionen (z.B. Alter, Einkommen, aber auch Vorlieben oder Konsumverhalten) klassifizieren kann. Selbst die Aufbewahrung von Daten, von denen man nicht weiss, wie man sie verwenden will, kann lukrativ sein, denn möglicherweise werden die Daten in Zukunft mit neu entwickelten Analysemöglichkeiten gewinnbringend bearbeitet werden können.

Für den Datenschutz stellt sich somit die Herausforderung, dass die heute zur Verfügung stehenden (und die für die Zukunft erwarteten oder noch nicht absehbaren) Möglichkeiten, Daten zu bearbeiten, für einen Teil der Datenbearbeiter keinen Anreiz zu einem sparsamen Umgang mit personenbezogenen Informationen bieten, sondern eher das Gegenteil zutrifft. Ein Beispiel dafür sind Soziale Netzwerke wie Facebook. Die dort bestehenden Austauschmöglichkeiten über persönliche Vorlieben erlauben weit gehende Rückschlüsse über die Präferenzen der Nutzerinnen und Nutzer, die somit zielgruppengerecht beworben werden können. Gleichzeitig sind die Einstellungen bei diesen Netzwerken häufig auf eine grosse Zugänglichkeit der eingegebenen Daten voreingestellt und müssen manuell geändert werden (Opt-out-Prinzip; Fraunhofer Institut 2008).

Bundesorgane

Auch für staatliche Stellen ergeben sich Konsequenzen aus neuen Technologien und Anwendungen: Auffällige Entwicklungen betreffen den Sicherheitsbereich (elektronische Fahndung, Datenbanken, auch biometrischer Pass). Grundsätzlich ist es auch in diesem Bereich möglich, grosse Mengen an Informationen zu generieren, festzuhalten und zu verknüpfen. Ebenso ermöglichen die verbesserten technischen Systeme einen erleichterten Austausch von Personendaten zwischen verschiedenen Behörden, was bei der Prüfung des rechtmässigen Bezugs von staatlichen Leistungen genutzt wird (vgl. dazu Bolliger/Féraud 2010). In den Interviews wurde teilweise erwähnt, dass im staatlichen Bereich der erleichterten Generierung und Speicherung personenbezogener Informationen im Zuge einer unkontrollierten Ausnutzung der neuen technologischen Möglichkeiten durch das Legalitätsprinzip Schranken gesetzt werden.

4.1.2 Sachbereiche mit Herausforderungen: Einschätzungen der Experten

Eine Mehrheit der Befragten gibt zu bedenken, dass die genannten technologischen Entwicklungen (vgl. Kapitel 3) grundsätzlich in den verschiedensten staatlichen und privaten Bereichen zu Herausforderungen für den Datenschutz führen können. Dies dürfte insbesondere dann zutreffen, wenn ein Bereich zunehmend von der Digitalisierung betroffen ist, was gemäss verschiedenen Einschätzungen für die unterschiedlichsten Bereiche zutreffe.

Ein Teil der Befragten sieht die grössten Probleme im Privatbereich. Dabei gilt es nicht nur zu beachten, wie mit eigenen Daten umgegangen werde, sondern auch das Problem, dass durch die Veröffentlichung von Bildern und Videos auch die Privatsphäre Dritter verletzt werden könne (z.B. Facebook, Youtube).

Als heikel wird von verschiedenen Seiten der Umgang mit Gesundheitsdaten (Gesundheits- und Versicherungsbereich) bezeichnet. Nebst der Tatsache, dass es sich dabei gemäss dem DSG um besonders schützenswerte Personendaten handelt und der zunehmenden Digitalisierung (E-Health) in diesem Bereich, dürfte auch die besondere Akteurskonstellation zwischen Leistungserbringer, Versicherer sowie Patient/Versicherter mit jeweils unterschiedlichen Interessen zur kritischen Einschätzung beigetragen haben. In einem Interview wurde darauf hingewiesen, dass im Arbeitsbereich aufgrund der hierarchischen Beziehung zwischen Arbeitgeber und Arbeitnehmer besondere Hürden für Betroffene entstehen können. Am Gesundheits- und am Arbeitsbereich zeigt es sich, dass auch in eher klassischen Konstellationen nach wie vor als bedeutend einzustufende Datenschutz-Risiken bestehen dürften.

Als letzter Punkt kann die Herausforderung der Datenverknüpfungen genannt werden. So können an sich eher unproblematische Informationen wie die von einem Detailhändler erhobenen Daten zum Kaufverhalten eines Kunden dann heikel werden, wenn sie von einer Krankenversicherung dazu verwendet werden, die Prämien für den Versicherten unter Berücksichtigung der Kaufgewohnheiten anzupassen. Mögliche Verknüpfungen von Personendaten aus verschiedenen Bereichen werden jedoch nicht durchwegs als problematisch eingestuft. In Einzelfällen, im Besonderen bei der Aufklärung von Verbrechen, kann es laut Interviewpartnern durchaus legitim sein, Daten entgegen ihrem ursprünglichen Zweck zu bearbeiten.

4.1.3 Sachbereiche mit Herausforderungen: Quantitative Auswertungen

Ergänzend wurde eine überwiegend quantitative Analyse der juristischen Bibliographie des Bundesgerichts aus den Jahren 2003 bis 2010 (Bundesgericht 2003a ff.; 2003b ff.) sowie der Schwerpunktsetzung der Zeitschrift „digma“ aus den Jahren 2001 bis 2010 (Digma 2001 ff.) durchgeführt, um zu zeigen, welche Gebiete Fachleute des Datenschutzes hauptsächlich thematisieren. Ebenfalls berücksichtigt und thematisch zugeordnet wurden die im National- und Ständerat eingereichten Vorstösse mit datenschutzrechtlicher Relevanz[8]. Während die Publikationen im Bereich Datenschutz Hinweise auf Problemfelder aus Sicht von Experten geben können, deuten die Vorstösse im Parlament darauf hin, was Politiker und damit Vertreter der Öffentlichkeit als wichtig erachten.

Im *Internet- und Telekommunikationsbereich* befassen sich verschiedene digma-Ausgaben schwerpunktmässig mit Themen aus dem Bereich Internet und Telekommunikation. Themen sind u.a. Google Street View, Cloud Computing, Cyber Ermittlungen, Mobile Dienste, Pervasive Computing. Sie nehmen damit teilweise Bezug auf die im vorigen Kapitel beschriebenen allgemeineren Entwicklungen im Technologiebereich. Bei den parlamentarischen Vorstössen fällt auf, dass die

[8] Geschäfts-Datenbank Curia Vista: http://www.parlament.ch/d/dokumentation/curia-vista/Seiten/default.aspx; 31.1.2011.

missbräuchliche Verwendung des Internets (Stichwort Internetkriminalität) ein grösseres Gewicht hat als in den ausgewerteten Publikationen.

Die Veröffentlichungen, die zum Bereich *Justiz, Polizei und Sicherheit* gezählt wurden, umfassen die Themen Datenschutz im Rahmen von polizeilichen Ermittlungen und im Strafprozessrecht, Schengen (insbesondere SIS) sowie Überwachungsstaat und Staatsschutz. Ebenfalls prominent thematisiert werden unterschiedliche Datenbanken (DNA-, Hooligan-, polizeiliche Datenbanken, SIS). Digma hat sich mit Themen Überwachungsstaat/Staatsschutz und Hooliganismus beschäftigt. Bei den parlamentarischen Vorstössen finden sich unter anderem die Themen Überwachung mittels Drohnen, Datenweitergabe an US-Behörden im Rahmen der Terrorismusbekämpfung, Datenbearbeitungen im Zusammenhang mit der inneren Sicherheit sowie Datenbanken.

Der Fokus der juristischen Literatur im *Gesundheitsbereich* liegt auf Datenschutzfragen im Zusammenhang mit Patientendaten. Zu erwähnen gilt es insbesondere die *Gesundheitskarte* und *E-Health* (zu beiden Themen wurde eine Digma-Sondernummer veröffentlicht) sowie den Umgang mit genetischen Daten. Ein Digma-Heft beschäftigt sich mit datenschutzrelevanten Herausforderungen im Pharmabereich. Die Versichertenkarte und E-Health spielen auch im Rahmen von parlamentarischen Vorstössen eine Rolle.

Ein grosser Teil der Publikationen zum *Versicherungsbereich* befasst sich recht allgemein mit dem Thema Versicherungen und Datenschutz. Eine gewisse Brisanz wird möglicherweise in der Rolle des Vertrauensarztes gesehen (zwei Beiträge). Kritisch beurteilt wird im Rahmen von parlamentarischen Vorstössen der Datenschutz bei den Krankenversicherungen (Datenaustausch Leistungserbringer-Versicherer; Auslagerung der Datenbearbeitung; Case Management; Zugriffsmöglichkeiten auf sensible medizinische Daten), auf die sich die meisten Geschäfte beziehen.

Die Beiträge in der juristischen Literatur im Bereich *Handel und Wirtschaft* befassen sich schwerpunktmässig mit der Rolle des Datenschutzes im Zusammenhang mit Fusionen, dem IT-Outsourcing sowie Standards und Zertifizierungen. Spezifischere, datenschutzrelevante Anwendungsbeispiele könnten Records Management, Assessment Center sowie Customer Relationship Management sein. Verschiedene Themen wurden auch von digma aufgenommen. Im Parlament sind Vorstösse auf diesem Gebiet rar.

Im *Arbeitsbereich* nehmen die Überwachung am Arbeitsplatz sowie der Umgang mit Gesundheitsdaten der Arbeitnehmenden (Arztzeugnisse, Datenweitergabe an Versicherungen) neben allgemeinen Publikationen zum Datenschutz im Arbeitsrecht eine wichtige Rolle ein. Die erste digma-Ausgabe aus dem Jahr 2001 befasst sich zudem mit dem Thema „Internet am Arbeitsplatz“ und befasst sich dabei auch mit der Frage der Überwachung. Im Parlament sind Vorstösse auf diesem Gebiet rar (zwei zur Überwachung am Arbeitsplatz).

Im *Finanzbereich* lassen sich in der Literatur zwei Schwerpunkte finden: Der eine beschäftigt sich mit der Bekanntgabe von Bankkundendaten, der andere mit dem Scoring bei der Vergabe von Krediten (Digma-Sonderheft 2007). Die Mehrheit der parlamentarischen Vorstösse bezieht sich auf das Bankgeheimnis. Eine Petition fordert die Verankerung des Bankkundengeheimnisses im DSG. Daneben spielt die Datenbekanntgabe ins Ausland (Swift) in zwei Fällen eine Rolle.

Im *Technologiebereich* schliesslich werden die Videoüberwachung und der Einsatz von Biometrie diskutiert (diverse Publikationen; jeweils Schwerpunkt in digma). Auch im Parlament wurden diese Techniken berücksichtigt. Die Biometrie war vor allem mit der Einführung von biometrischen Ausweisen ein Thema; in den entsprechenden Vorstössen wird eine skeptische Haltung zum Ausdruck gebracht, vor allem was die Sicherheitsrisiken und die Zuverlässigkeit angeht. Daneben waren die Videoüberwachung und die RFID-Technologie Gegenstände von Vorstössen, in einem Fall auch drahtlose Netzwerke.

Insgesamt zeigt sich eine grosse Breite an Anwendungsfeldern, in denen der Datenschutz von Politik und Experten als wichtiges Thema erachtet wird. Eine Reduktion auf einzelne Problemfelder ist kaum möglich.

4.2 Einhaltung der gesetzlichen Vorgaben durch die Datenbearbeiter

In diesem Abschnitt wird die Einhaltung des Datenschutzgesetzes durch öffentliche und private Datenbearbeiter näher untersucht. Zunächst wird allgemein darauf eingegangen, welche empirische Evidenz insgesamt zur Einhaltung des DSG durch die Datenbearbeiter vorhanden ist. Anschliessend werden für private und öffentliche Datenbearbeiter Anreizstrukturen, welche deren Verhalten mit beeinflussen, diskutiert. Schliesslich befasst sich dieser Abschnitt mit Aspekten der Umsetzung sowie der Ausbildung im Datenschutzbereich.

4.2.1 Einhaltung der gesetzlichen Vorgaben: Allgemeine Einschätzungen

Im Folgenden gehen wir zunächst allgemein auf Einschätzungen der Interviewpartner zur Umsetzung des DSG in der Bundesverwaltung und in der Privatwirtschaft ein. Gemäss einem Rechtsexperten ist die Einhaltung der Datenschutzvorschriften in der Bundesverwaltung als gut zu bezeichnen. Insgesamt weisen die Interviewaussagen in die Richtung, dass Bundesorgane den Datenschutz insgesamt eher besser berücksichtigen als private Akteure. Seitens der Interviewpartner beim EDÖB wird die Situation nuancierter wahrgenommen: Bei den Bundesorganen stellen sie eine grosse Heterogenität zwischen den Departementen und Ämtern bezüglich der Bedeutung des Datenschutzes fest.

Gemäss einem Interviewpartner gibt es in der Schweiz keine Unternehmung, die das DSG vollständig einhalten würde. Es gebe aber sehr viele Firmen, die versuchen würden, sich gemäss den Vorschriften zu verhalten, und dies trotz des geringen Risikos, im Falle einer Verletzung des DSG sanktioniert zu werden. Insgesamt kommen verschiedene Interviewpartner zum Schluss, dass es für grössere Unternehmen, die aufgrund ihrer Bekanntheit im Fokus der Öffentlichkeit stehen, wichtiger sei als für andere, dem Datenschutz zu genügen. Für die meisten Unternehmen reiche es aus, mit dem allgemeinen Strom zu schwimmen und keine gravierenden Datenschutzverletzungen zuzulassen. Diesen Eindruck bestätigten im Interview auch die befragten Mitarbeiter des EDÖB.

Die Datenbearbeiter selber wurden nicht direkt gefragt, ob sie ihre Pflichten gemäss dem DSG erfüllen. Aus den Interviews haben sich jedoch Hinweise gegeben, die den Einschätzungen der Experten und Interessenvertreter zumindest nicht widersprechen. So wurde im Privatbereich

insbesondere darauf aufmerksam gemacht, dass der Datenschutz einer von verschiedenen Aspekten sei, den eine Unternehmung bei ihren Entscheidungen zu berücksichtigen habe. Dabei werde eine Abwägung gemacht und nicht immer die aus Datenschutzsicht vorzuziehende Variante gewählt.

In den Gesprächen mit Datenbearbeitern aus der Bundesverwaltung wurde demgegenüber auf das generell geltende und auch im Datenschutzgesetz explizit verankerte Legalitätsprinzip verwiesen: Art. 17 Abs. 1 DSG verlangt, dass sämtliches Verwaltungshandeln auf einer Rechtsgrundlage beruht (Rosenthal/Jöhri 2008: 457ff.). Dies schliesst zwar nicht aus, dass Personendaten in der Bundesverwaltung widerrechtlich bearbeitet werden, setze jedoch dem staatlichen Handeln gegenüber dem Privatbereich engere Grenzen.

Hinweise auf die Einhaltung des DSG durch die privaten Datenbearbeiter und Bundesorgane lassen sich darüber hinaus aus anderen empirischen Erkenntnissen dieser Evaluation ziehen: So gaben im Rahmen der Bevölkerungsumfrage rund 20% der Befragten an, schon einmal von einem Missbrauch ihrer Daten betroffen gewesen zu sein (vgl. Ziffer 8.2.1). Auch im Rahmen der Fallstudien und der Analyse der Aktivitäten des EDÖB zeigt sich, dass es in der Praxis zu Datenschutzverletzungen kommt (vgl. Kapitel 12). Somit lässt sich bilanzieren, dass die Datenschutzbestimmungen in der Praxis nicht immer eingehalten werden. Quantifizieren lässt sich die unrechtmässige Bearbeitung von Daten nicht, da – insbesondere in den neuen, unübersichtlichen Formen der Datenbearbeitung – viele solcher Missbräuche unentdeckt bleiben dürften.

4.2.2 Anreize zur Beachtung des Datenschutzes für Unternehmen

Es gibt verschiedene Risiken, die Unternehmen (auch solche, die gemäss dem Datenschutz als Bundesorgane gelten wie beispielsweise die obligatorischen Krankenversicherer oder die Pensionskassen) einen Anreiz zur Berücksichtigung der datenschutzrechtlichen Bestimmungen geben können (Tabelle 4-1): Das Sanktionsrisiko, das Imagerisiko und das Investitionsrisiko. Deren Bedeutung wurde von den Interviewpartnern als unterschiedlich gross beurteilt. Sie liefern eine mögliche Begründung für den Eindruck der Befragten, wonach die Mehrheit der Unternehmen zwar nicht alle Bestimmungen des DSG strikt einhält, schwerwiegende Datenschutzverletzungen aber dennoch selten seien.

Tabelle 4-1 zeigt, dass die Interviewpartner (auch jene beim EDÖB) das Sanktionsrisiko für Unternehmen als eher gering beurteilen. Dies wird einerseits damit begründet, dass die Durchsetzungsmechanismen als zu schwach betrachtet werden: Die Durchsetzung auf dem Gerichtsweg stelle für die betroffene Person eine sehr hohe Hürde dar, und der EDÖB in seiner Funktion als Aufsichtsorgan könne mangels Ressourcen nur die wenigsten Fälle effektiv abklären. Auch die Sanktionen im DSG werden als schwach bezeichnet, so dass von ihnen kaum ein Anreiz ausgehe, sich gesetzeskonform zu verhalten.

Demgegenüber besteht, insbesondere für grosse Unternehmen, die in der Öffentlichkeit stehen, im Falle gravierender Datenschutzverletzungen gemäss den Gesprächsaussagen ein beträchtliches Imagerisiko, welches sie dazu bewegt, datenschutzrechtlichen Aspekten ein bestimmtes Gewicht beizumessen. Dieser Punkt zeigt sich auch in der Einschätzung der meisten Bearbeiter, dass der

Datenschutz zum Vertrauen der Kundinnen und Kunden in das Unternehmen einen Beitrag leisten oder ein Marketingargument sein könne. In die gleiche Richtung deuten auch die Aussagen der Interviewpartner beim EDÖB (allgemein und im Rahmen der Fallstudien); hier wird festgestellt, dass Empfehlungen von den betroffenen Bearbeitern als schmerzhaft empfunden würden, obwohl sie keine unmittelbare Rechtskraft entfalteten. Auch die konsequente Veröffentlichung von Empfehlungen durch den EDÖB erscheint vor diesem Hintergrund als wirksame Vorgehensweise.

Tabelle 4-1: Risiken für private Unternehmen bei Datenschutzverletzungen

Risikoart	*Beschreibung*	*Beurteilung durch Interviewpartner*
Sanktionsrisiko	Wahrscheinlichkeit, dass eine Datenschutzverletzung durch ein Unternehmen rechtliche Folgen nach sich zieht.	Tief: Die Wahrscheinlichkeit, dass ein Vergehen geahndet wird, wird als tief beurteilt, die Strenge einer allfälligen Strafe als gering.
Imagerisiko	Schaden der entsteht, wenn ein Unternehmen durch eine Datenschutzverletzung negative Schlagzeilen in der Öffentlichkeit macht.	Gravierend, wenn ein aufsehenerregender Fall ans Licht kommt; besonders für bekannte Firmen.
Investitionsrisiko	Wahrscheinlichkeit, dass ein neues Produkt aus datenschutzrechtlichen Gründen verboten wird.	Risiko wird als klein beurteilt, Schaden ist aber im Einzelfall gross.

Vom Investitionsrisiko schliesslich kann in einzelnen Fällen ebenfalls der Anreiz ausgehen, grobe Regelverstösse zu unterlassen. In einer Fallstudie zu einer Sachverhaltsabklärung (vgl. Fallstudien im Anhang 4), in welcher der EDÖB eine Datenbearbeitung mittels einer provisorischen Massnahme verlangte, hat sich gezeigt, dass das Image- und auch das Investitionsrisiko für die Bearbeiter durchaus von Bedeutung sind.

4.2.3 Anreizstrukturen bei Bundesbehörden

Die Ergebnisse aus dem Privatbereich lassen sich nicht ohne weiteres auf die Bearbeitung von Personendaten durch Bundesorgane übertragen; teilweise lassen sich jedoch analoge Überlegungen anstellen. Bezüglich des Sanktionsrisikos befinden sich Bundesbehörden in einer ähnlichen Situation wie private Bearbeiter: Die Wahrscheinlichkeit, sanktioniert zu werden, kann für Bundesorgane ähnlich wie für die privaten Akteure als nicht sehr hoch beurteilt werden. Die Interviewpartner der befragten öffentlich-rechtlichen Datenbearbeiter gaben an, sie spürten faktisch wenig von der Aufsichtsfunktion des EDÖB; sie vermuten, dass dieser Umstand mit der Ressourcensituation beim EDÖB zusammenhänge.

Das Image- und das Investitionsrisiko lassen sich kaum auf die Tätigkeit von Bundesorganen im engeren Sinn (innerhalb der Bundesverwaltung) übertragen. Ein wichtiger Faktor dürfte dagegen das intakte Vertrauen der Bürgerinnen und Bürger in die Personendaten bearbeitenden staatlichen Stellen sein. Alle drei befragten Datenbearbeiter gaben diesbezüglich an, dass die Einhaltung des DSG auch unter diesem Gesichtspunkt von grosser Bedeutung für das jeweilige Amt resp.

Departement sei; in der Fallstudie zur *Schweizerischen Arbeitskräfteerhebung (SAKE*, vgl. Anhang 4) argumentierte der EDÖB gegenüber dem Bundesamt für Statistik, dass das BFS bei seiner Befragung auf das Vertrauen der Bevölkerung angewiesen sei, wenn es verlässliche Umfrageergebnisse erzielen wolle. Er schlägt dabei unter anderem vor, dass im Informationsschreiben des BFS an die befragten Bürgerinnen und Bürger ein Identifikationscode aufgeführt wird, der es den Befragten ermöglicht, das mit der Befragung beauftragte private Umfrageinstitut zu authentifizieren. Nach Aussagen von EDÖB-Mitarbeitern erkennen die Privatunternehmen die Risiken, die sich für sie aus der Missachtung von Prinzipien des Datenschutzes ergeben, tendenziell schneller als die Bundesverwaltung. Umgekehrt wirkt bei den Bundesorganen dafür mit dem Legalitätsprinzip ein Mechanismus zugunsten des Datenschutzes, der bei den Privaten wegfällt.

4.2.4 Umsetzung der Datenschutzbestimmungen: Massnahmen und Aufwand

Datenbearbeiter treffen unterschiedliche Massnahmen auf verschiedenen Ebenen, um den Datenschutz in ihrem Unternehmen oder in ihrem Amt oder Departement umzusetzen.

- *Betriebliche Datenschutzverantwortliche / Datenschutzberater:* In der Mehrheit der Unternehmen, die im Rahmen dieser Studie befragt worden sind, wurde die Stelle der betrieblichen Datenschutzverantwortlichen geschaffen. Den eigenen Aussagen zu Folge wird dies als wichtige Massnahme erachtet, um die Bestimmungen des DSG umsetzen zu können. Auch beim EDÖB wird begrüsst, dass einige Unternehmen Datenschutzveranwortliche eingesetzt werden. Da gemäss dem DSG aber keine Verpflichtung für die Schaffung einer solchen Stelle besteht, sondern das DSG (in Art. 11a Abs. 5 Buchstabe e) diese lediglich freiwillig vorsieht, beschränkt sich diese Feststellung auf grössere Unternehmen. Bei den KMU stellen die befragten EDÖB-Mitarbeiter in dieser Beziehung kaum Bewegung fest. In den Ämtern der Bundesverwaltung wurden verschiedentlich ebenfalls Datenschutzberater eingesetzt. Daneben hat jedes Departement einen Datenschutzverantwortlichen (Art 23 VDSG). Die befragten EDÖB-Mitarbeiter orten jedoch beim Bund noch verschiedene Verbesserungspotenziale und bedeutende Unterschiede bezüglich der Verankerung des Datenschutzes (vgl. Ziffer 11.4.4).

- *Ausbildung der Mitarbeiterinnen und Mitarbeiter:* Eine wichtige Massnahme für die Einhaltung der Datenschutzgrundsätze sehen die Befragten in der Ausbildung der übrigen Mitarbeiter, wobei in diesem Zusammenhang unterschiedliche Instrumente zur Anwendung kommen (Einführung bei Stellenantritt, Schulungen, webbasiertes Training, Beratung). Auch durch formelle Bestimmungen (Schweigepflicht, Reglemente, Weisungen an Mitarbeiter) oder die Definition von Zugriffsrechten wird dafür gesorgt, dass der Datenschutz eingehalten werden kann.

- *Technische Sicherheit:* Ein weiteres Standbein bei der Umsetzung der Datenschutzgrundsätze ist die Gewährleistung der technischen Sicherheit. Nebst der engen Zusammenarbeit mit den jeweiligen IT-Abteilungen gilt es insbesondere bei der Einführung neuer Projekte, Produkte und Dienstleistungen zu prüfen, dass dem Datenschutz genüge getragen wird. Dies wird in der Bundesverwaltung mit Hilfe der Projektführungsmethode Hermes gewährleistet, was gemäss den Interviewaussagen dazu führt, dass Datenschutzaspekte ausreichend berücksich-

tigt werden (vgl. auch EFK 2007). Die Befragten beim EDÖB bemängeln eine angeblich inkonsequente Umsetzung der Vorgaben von Hermes in der Bundesverwaltung bemängelt. Auch die Datenschutzverantwortlichen im Privatbereich werden bei IT-Projekten konsultiert, scheinen aber in einigen Fällen Mühe zu haben, ein hohes Datenschutzniveau in den Projekten zu sichern.

- *Datenschutzaudits, Zertifizierung:* Schliesslich kann die Überprüfung des Datenschutzes durch interne Kontrollen oder Audits überprüft werden. Einige Unternehmen verfügen über das Zertifikat „Good Privacy". Aussagen über die Wirkung der gesetzlich neu eingeführten Zertifikate (Art. 11 DSG) sind noch nicht möglich.

Der Aufwand, der für die Datenbearbeiter zur Einhaltung der Datenschutzgrundsätze entsteht, ist laut Einschätzung der Befragten vertretbar. Bei einem Teil der Befragten machen Datenschutzthemen weniger als 20% der gesamten Tätigkeit einer Person aus. Als positiv hervorgehoben wird seitens der Datenbearbeiter, dass der durch die Datenschutzgesetzgebung entstehende Aufwand kleiner sei als in anderen Ländern (insbesondere Deutschland).

4.2.5 Umsetzung der Datenschutzbestimmungen: Probleme

Die Datenbearbeiter wurden nach den Problemen gefragt, die sich im Zusammenhang mit der Umsetzung des DSG allenfalls ergeben. Eine Mehrheit der Befragten weist darauf hin, dass die Umsetzung des DSG nicht zu grösseren Problemen geführt habe. Dennoch sind einige Punkte vor allem aus dem Privatbereich erwähnt worden:

- *Fehlende konkrete Handlungsanleitungen:* Sowohl von privater und von öffentlicher Seite ist angeführt worden, dass das DSG als Rahmengesetz sehr allgemein formuliert sei und so im Alltag der Datenbearbeiter oftmals nicht weiterhelfe. Konkretisierungen (Präzedenzfälle, Richtlinien des EDÖB) seien häufig nicht vorhanden.

- *Aufwand für Kunden durch Datenschutz:* Ebenfalls erwähnt worden ist, dass der Datenschutz allenfalls mit anderen Zielsetzungen kollidieren könne. So könne bei der Sicherstellung der Einwilligung in die Datenbearbeitung für den Kunden ein unverhältnismässig grosser Aufwand entstehen, der sich negativ auf die Kundenzufriedenheit auswirke. Die Bearbeiter befinden sich in dieser Situation den Interviewaussagen zufolge in einem Dilemma: Würden die Prozesse kundenfreundlich gestaltet, könne dies Datenschutzverletzungen hervorrufen, während die Einhaltung der Datenschutzvorschriften zu wenig kundenfreundlichen Abläufen führen könne.

- *Fehlende gesetzliche Grundlage:* Seitens der Datenbearbeiter aus der Bundesverwaltung wurde erwähnt, dass die häufigste Problematik eine fehlende oder ungenügende gesetzliche Grundlage sei. Hier wurde von einer Person angemerkt, die rechtlichen Grundlagen hinkten immer der technologischen Entwicklung hinterher.

Insgesamt kann basierend auf den Aussagen der interviewten Bearbeiter trotz der erwähnten teilweise auch kritischen Punkte bilanziert werden, dass diese in der Regel für in der Praxis anfallende Problemsituationen Lösungen finden. Dass sie aufgrund des DSG eine Datenbearbeitung

stark einschränken oder gar darauf verzichten, kommt offenbar selten vor. Dagegen müssen die betrieblichen Datenschutzverantwortlichen und die Datenschutzberater des Bundes im Rahmen der Prüfung von IT-Projekten ihren Aussagen zufolge öfters darauf hinweisen, dass eine bestimmte Bearbeitung anders ausgestaltet werden müsse (Zugriffsrechte, technische Sicherheit, Anonymisierung, Umfang erhobener Informationen). Die Aussagen der Bearbeiter zu den Problemen bei der Umsetzung deuten auf einen insgesamt pragmatischen Umgang mit den Vorschriften des DSG hin.

4.2.6 Ausbildung und Ausbildungsmöglichkeiten

Sämtliche interviewten Vertreter (überwiegend Juristen) von Datenbearbeitern haben ihre Datenschutzkenntnisse auf verschiedenen Kanälen erworben. Alle Interviewpartner betonen als wichtigste Quelle die Erfahrungen im Rahmen der täglichen Arbeit (Ausbildung on the job, learning by doing). Dies wird als besonders wichtig eingestuft, da jede Branche mit unterschiedlichen, spezifischen Datenschutzfragen zu tun habe, die nur sehr schwer im Rahmen anderer Ausbildungsmöglichkeiten (z.B. Kurse, Tagungen) ausgiebig erörtert werden könnten. Eine zweite Möglichkeit, sich die notwendigen Erkenntnisse im Datenschutzbereich anzueignen, ist der Besuch von Tagungen oder Weiterbildungen in der Schweiz und in Einzelfällen auch im Ausland. Am häufigsten genannt wird in diesem Zusammenhang das Datenschutzforum Schweiz, welches Aus- und Weiterbildungen auf dem Gebiet des Datenschutzes und der Datensicherheit bereitstellt und sowohl für Bundesvertreter wie auch Datenbearbeiter aus der Privatwirtschaft Kurse bereithält. Daneben existieren noch weitere Angebote, wie der von der Universität Freiburg, dem EDÖB und dem Verein Privatim organisierte Schweizerische Datenschutzrechtstag und Weiterbildungstage oder Veranstaltungen von Verbänden und Privaten, wie z.B. Anwaltskanzleien.

Schliesslich wurde drittens der Austausch mit anderen Datenschutzverantwortlichen als weitere Möglichkeit genannt, insbesondere praxisnahe Probleme bilateral oder in einem grösseren Gremium zu erörtern. Im Privatbereich kann diesbezüglich dem Verein Unternehmensdatenschutz (VUD) eine besondere Bedeutung beigemessen werden: Die privaten Datenbearbeiter bezeichnen den Verein als sehr sinnvolles Gefäss zum Informations- und Erfahrungsaustausch sowie zur Diskussion von konkreten, datenschutzrelevanten Fragestellungen. Von praktisch allen Befragten, die im VUD vertreten sind, wird der Verein als wertvoller eingeschätzt als die übrigen Ausbildungsmöglichkeiten. In der französischen Schweiz sich hat kürzlich ein ähnlicher Verein konstituiert (Association des Professionnels de la Protection des données, APPD).

Insgesamt wird von den Befragten das Ausbildungsangebot in der Schweiz als sehr schmal empfunden. Die Qualität der existierenden Veranstaltungen wird teilweise bemängelt: Sie sei zu allgemein und mit einem geringen Nutzen für die branchenspezifischen Fragestellungen im Alltagsgeschäft. Unterschiedlich fällt die Bewertung der Tatsache aus, dass die Aus- und Weiterbildungsmöglichkeiten eher gering sind.

Von den befragten Vertretern von Bundesorganen ist teilweise erwähnt worden, dass mehr Aus- und Weiterbildungsmöglichkeiten (speziell für die Bundesverwaltung) erwünscht wären, und sie sehen dabei auch den EDÖB in einer wichtigen Rolle, beispielsweise in der Bereitstellung von Ausbildungsinhalten. Der Wunsch nach spezifischen Ausbildungsangeboten des EDÖB zuhan-

den der Datenschutzberater des Bundes ist bereits im Rahmen früherer Untersuchungen aufgebracht worden (GPK-N 2003: 1422; EFK 2007). Entsprechende Unterlagen hat der EDÖB unterdessen bereitgestellt. Ergänzend ist die im Auftrag des EDÖB erstellte Publikation *„Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben"* (Epiney/Civitella/Zbinden 2009) erarbeitet worden. Gemeinsam mit dem Verband Privatim und dem Institut für Europarecht der Universität Freiburg bietet der EDÖB seit 2008 zudem Weiterbildungsnachmittage an, die sich teilweise spezifisch an die Datenschutzberater in der Bundesverwaltung richten, andere Weiterbildungsveranstaltungen sind für andere Interessierte offen. Zu erwähnen ist auch die jährlich stattfindende Datenschutzrechtstagung (http://www.unifr.ch/euroinstitut/de). Inwieweit die Inhalte dieser Angebote den Wünschen den Datenschutzberatern des Bundes entsprechen, ist im Rahmen dieser Untersuchung nicht evaluiert worden. Im Privatbereich dagegen zeigten sich die Befragten skeptisch, ob es überhaupt möglich oder nötig sei, eine Ausbildung so zu gestalten, dass sie wirklich auf das Alltagsgeschäft in einer bestimmten Branche vorbereiten könne.

5 Sensibilität der Bevölkerung

Dieses Kapitel beschäftigt sich mit der Frage, wie sensibilisiert die Bevölkerung gegenüber der Bearbeitung von Personendaten durch private und öffentliche Stellen ist. Dabei werden wir im Folgenden die bei der Herleitung des Wirkungsmodells (vgl. Kapitel 2) diskutierten Dimensionen der Sensibilität der betroffenen Personen untersuchen, d.h. Einstellungen, Kenntnisse und Angaben über das Verhalten in Situationen, in denen der Datenschutz eine Rolle spielt.[9] Die Auseinandersetzung mit der Sensibilität der Bevölkerung zum Thema Datenschutz ist vor allem auch vor dem Hintergrund der Entwicklungen seit der Einführung des DSG von Interesse: Während im Vorfeld der Verabschiedung des Gesetzes durch die eidgenössischen Räte der „Fichenskandal" ein dominierendes politisches Thema war, stellt sich heute im Zeitalter des Internets und weltweiter Kommunikationsmöglichkeiten die Frage, inwiefern der Datenschutz überhaupt noch einem Bedürfnis der Bevölkerung entspricht, und inwieweit er als störendes Hindernis des freien Informationsflusses wahrgenommen wird. Auch die Frage, wie gut sich die Betroffenen in der Lage sehen, sich in dieser neuen Situation selbst vor missbräuchlichen Datenbearbeitungen zu schützen, wird thematisiert.

Die Evaluation stützt sich in diesem Kapitel überwiegend auf die Ergebnisse der durchgeführten Bevölkerungsbefragung bei 1014 im Rahmen einer geschichteten Zufallsstichprobe ausgewählten Personen (vgl. technische Informationen in Anhang 3). Punktuell und ergänzend wird auch auf Einschätzungen der befragten Experten, Interessenvertreter, Datenbearbeiter und der EDÖB-Mitarbeiterinnen und -Mitarbeiter Bezug genommen. Die Einschätzungen der Interviewpartner können dabei in doppelter Hinsicht von Interesse sein: Zum einen können sie Erklärungen für bestimmte Muster, die sich aus Bevölkerungsbefragung ergeben haben, liefern und Zusammenhange verdeutlichen; zum anderen erlauben es die Gesprächsaussagen aber auch, die Selbstwahrnehmung der Teilnehmenden an der Umfrage kritisch zu hinterfragen. Ergänzt werden die Ausführungen durch die Ergebnisse anderer Umfragen (Eurobarometer 2008; Privatim 2009; Petersen 2010).

5.1 Wichtigkeit des Schutzes persönlicher Daten

Im Rahmen der Umfrage von Privatim zum Datenschutz gaben im Januar 2009 rund drei Viertel der Befragten an, dass es ihnen wichtig oder sehr wichtig sei, was mit persönlichen Daten von ihnen im Internet geschieht. Rund 90% der Befragten gaben an, es sei ihnen wichtig oder sehr wichtig, dass Unternehmen und Verwaltungen ihre persönlichen Daten schützten (Privatim 2009). Die Befragung zeigte, dass eine grosse Mehrheit Bevölkerung den Datenschutz als wichtiges Anliegen anerkennt.

Im Rahmen einer Umfrage in Deutschland im Sommer 2010 gaben 79% der Befragten an, sie machten sich etwas (60%) oder sehr (19%) darüber Sorgen, dass persönliche Daten missbraucht

[9] Weitere Ergebnisse der Befragung finden sich an anderer Stelle in diesem Bericht: Kenntnisse DSG und Verhalten in Missbrauchssituationen: vgl. Kapitel 8; Bekanntheit EDÖB: vgl. Ziffer 12.1.1.

würden (Petersen 2010). Gleichzeitig ergab sich jedoch aus dieser Umfrage, dass die Sorge um Datenmissbrauch im Vergleich zu anderen Sorgen der Bevölkerung von eher nachrangiger Bedeutung ist. In der jüngsten Eurobarometer-Umfrage von Januar 2008 zum Thema Datenschutz gaben knapp zwei Drittel der Befragten (EU-Bevölkerung) an, es sei ihnen ein Anliegen[10], dass Organisationen ihre Daten korrekt bearbeiten. Der Anteil schwankt je nach Land stark, von 36% in Finnland bis 86% in Deutschland und Österreich (Eurobarometer 2008: 7).

In der Privatim-Umfrage gaben gut drei Viertel der Befragten (77%) zu Protokoll, sie seien der Meinung, dass ihre Daten in der Schweiz im Allgemeinen gut geschützt seien. Dieses Vertrauen ist im internationalen Vergleich hoch. Nur knapp die Hälfte der EU-Bürger vertrat 2008 die Ansicht, ihre persönlichen Daten würden in ihrem Land gut geschützt, wobei auch hier die Zustimmungsrate zu dieser Aussage je nach Land stark schwankte (von 26% in Griechenland bis 86% in Dänemark). Aus den Ergebnissen lässt sich ablesen, dass die Schweizer Bevölkerung den Datenschutz im internationalen Vergleich wichtig findet und ein vergleichsweise hohes Vertrauen hat, dass ihre Daten gut geschützt werden.

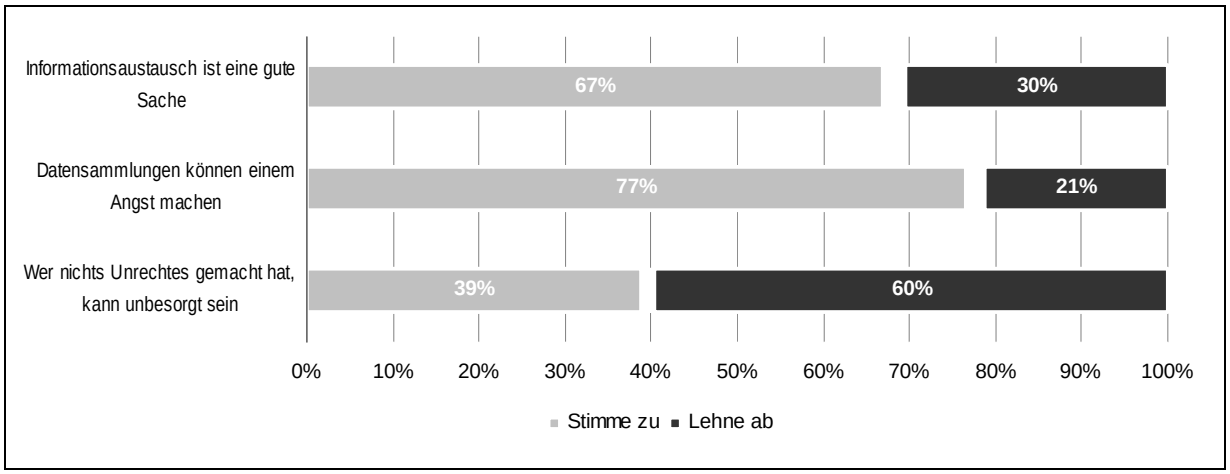
5.2 Informationszeitalter und allgegenwärtige Datenbearbeitungen

Im Rahmen der für diese Evaluation durchgeführten Umfrage kann dieses Bild ergänzt und verfeinert werden. Abbildung 5-1 zeigt die Antworten der Befragten zu verschiedenen Aussagen im Zusammenhang mit dem Informationsaustausch und dem Sammeln von Daten. Die Einstellungen der Bevölkerung zu den aktuellen Möglichkeiten des Informationsaustauschs und des Datensammelns sind ambivalent. Für zwei Drittel der Befragten überwiegen die positiven Seiten des Informationszeitalters. Sie stimmten der folgenden Aussage zu: „Dass man sich heutzutage mit anderen Menschen fast ständig und grenzenlos austauschen kann, ist eine gute Sache." Gleichzeitig hegt aber eine noch grössere Gruppe von Personen Bedenken gegenüber der Bearbeitung von Personendaten: 77% der Befragten stimmten der Aussage zu: „Die Vorstellung, wie viele Stellen heute Informationen über uns normale Leute sammeln und auswerten, kann einem Angst machen." [11]

[10] Die Frage lautete: "Different private and public organisations keep personal information about people. Are you concerned or not that your personal information is being protected by these organisations?"(Eurobarometer 2008: 7).

[11] Zu einem ähnlichen Schluss kommt Petersen (2010). In Deutschland gaben 75% der Befragten an, sie fänden es „unheimlich, wenn man hört, wo überall Daten von einem gespeichert werden, ohne dass man es weiss".

Abbildung 5-1: Einstellungen zu Informationsaustausch und Datensammlungen



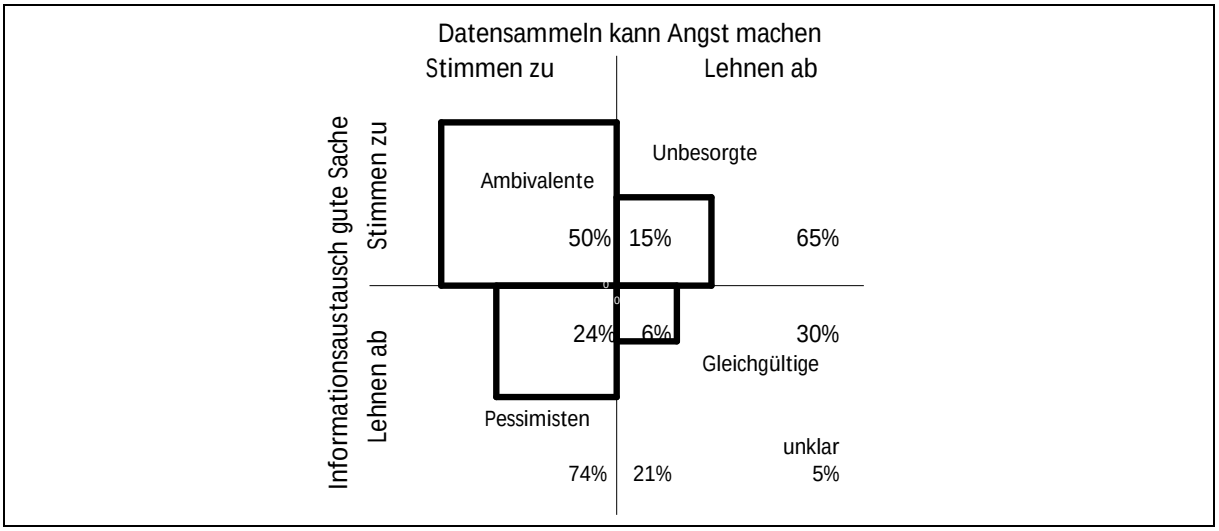
N = 1014. Der Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht“). Genaue Fragestellung vgl. Anhang 2.

Kombiniert man die Antworten zu diesen beiden Fragen, lassen sich unterschiedliche Typen bilden. Personen, die das Informationszeitalter befürworten und Datensammlungen nicht als potenziell Furcht einflössend empfinden, lassen sich zugespitzt als Unbesorgte bezeichnen. Pessimisten zeichnen sich demgegenüber durch eine Sorge über Datensammlungen und eine tendenzielle Ablehnung des Informationszeitalters aus. Personen, die zwar die Möglichkeiten des Informationsaustauschs begrüssen, sich aber über Datensammlungen Sorgen machen, lassen sich als Ambivalente umschreiben. Personen, die das Informationszeitalter ablehnen, aber sich über Datensammlungen keine Sorgen machen, haben wir als gleichgültig bezeichnet.

Wie Abbildung 5-2 zeigt, ist die Gruppe der Ambivalenten deutlich am grössten. Blendet man die 5% nicht zuzuordnenden Personen aus, so empfindet die Hälfte der Befragten trotz einer positiven Einstellung zum Informationszeitalter Datensammlungen als durchaus Besorgnis erregend. Die Pessimistinnen und Pessimisten machen rund einen Viertel der zuordenbaren Befragten aus (24%), die Unbesorgten bilden mit 15% eine verhältnismässig kleine Gruppe. Nur eine sehr kleine Minderheit (6%) ist gegenüber dem Informationszeitalter ablehnend und empfindet Datensammlungen gleichzeitig als harmlos (Gleichgültige).

Die Ergebnisse aus den qualitativen Interviews untermauern diese Befunde teilweise: Zum Ausdruck kam in den Gesprächen vor allem ein zunehmender Wunsch von breiten Teilen der Bevölkerung nach modernen Kommunikationsmöglichkeiten; gleichzeitig stellen aber Experten und auch die Befragten beim EDÖB eine gewisse Sorglosigkeit im Umgang mit solchen Angeboten fest. In den hier gefundenen Umfrageresultaten zeigt sich jedoch eine solche Unbesorgtheit wie gesehen nur bei einer Minderheit der Bevölkerung. Ein etwas anderes Bild resultiert bei den Antworten zu einem Statement, das eine gewisse Sorglosigkeit im Umgang mit persönlichen Daten suggeriert: „Wer nichts Unrechtes gemacht hat, dem kann es egal sein, was Andere über einem erfahren und weiterverbreiten.“ 39% der Antwortenden stimmten dieser Aussage zu.

Abbildung 5-2: Einstellungstypen: Informationsaustausch und Datensammeln



N= 1014. Genaue Fragestellung vgl. Anhang 2. Die Abweichungen in den ausgewiesenen Prozentwerten im Vergleich zu Abbildung 5-1 ergeben sich aus der höheren Anzahl Fälle mit unklaren Antworten (Kategorie „weiss nicht" bei mindestens einer der beiden berücksichtigten Fragen).

5.3 Selbstschutz und Schutz durch eine unabhängige Stelle

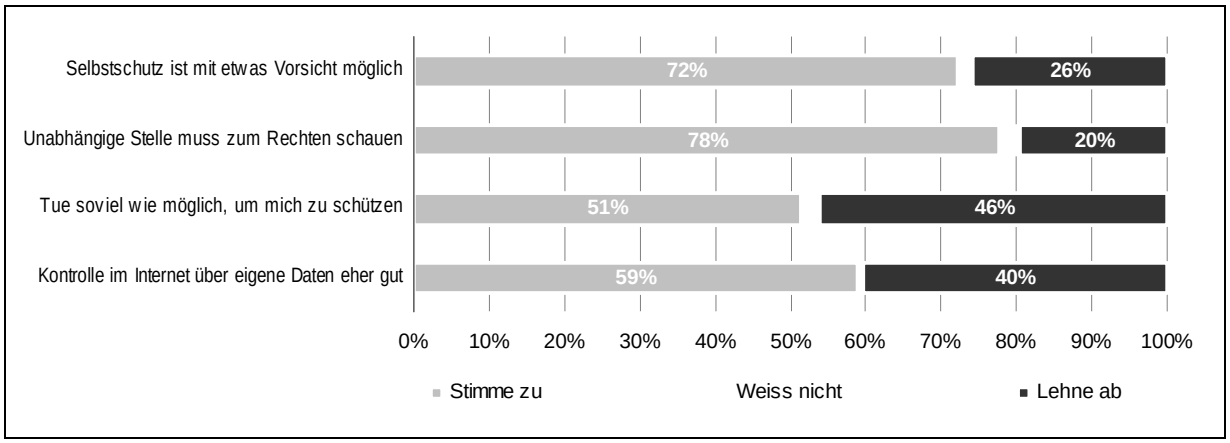
Eine deutliche Mehrheit der Befragten traut sich zu, die Kontrolle über die eigenen Personendaten selbst behalten zu können. Dies zeigt die Zustimmung von 72% zur Aussage: „Mit etwas Vorsicht kann man gut selber kontrollieren, dass persönliche Informationen über einem nicht in falsche Hände geraten" (Abbildung 5-3). Trotz dieses weit verbreiteten Zutrauens in die eigenen Fähigkeiten stimmt aber eine ebenso klare Mehrheit der Befragten einer unabhängigen Datenschutzstelle zu. Dies untermauern die 78% Zustimmung zur Aussage: „Es ist schwierig, unter Kontrolle zu behalten, was mit den persönlichen Angaben über einem passiert; deshalb muss eine unabhängige Stelle zum Rechten schauen." Ergänzend wurden die Umfrage-Teilnehmerinnen und -Teilnehmer zum Thema Selbstschutz befragt: „Glauben Sie, dass Sie sich selber so gut wie möglich vor Datenmissbrauch schützen, oder sind Sie unsicher, ob Sie diesbezüglich alles machen?" Rund die Hälfte der Antwortenden (51%) zeigte sich überzeugt, sich so gut wie möglich zu schützen, ein leicht geringerer Anteil von 46% zeigte sich diesbezüglich unsicher oder gab (selten) an, sich nicht zu schützen.

Schliesslich wurde spezifisch zu den Möglichkeiten des Selbstschutzes im Internet gefragt: „Wie ist Ihre Erfahrung, kann man im Internet als Einzelner eher gut oder eher schlecht selber bestimmen, welche Informationen über einem selbst für andere frei zugänglich sind und welche nicht?" Diese Frage, die nur den regelmässigen Internetnutzern[12] gestellt wurde, wurde von 59% mit eher ja oder ja beantwortet. Der Wert ist somit etwas tiefer als bei der allgemeinen Frage nach den Möglichkeiten, die Kontrolle über die Daten zu behalten. Jedoch sollte der Unterschied nicht überbewertet werden. Unter den Internetnutzern empfinden nicht 72% wie in der gesamten

[12] 822 von 1014 Personen gaben an, mindestens mehrmals pro Jahr das Internet zu nutzen; der grösste Teil davon gab an mehrmals pro Woche, fast täglich oder täglich im Internet zu sein.

Stichprobe, sondern nur 65% den Selbstschutz als gut möglich. Der verbleibende Unterschied kann auch an der Frageformulierung liegen.

Abbildung 5-3: Einstellungen zu Schutzmöglichkeiten vor Datenmissbrauch

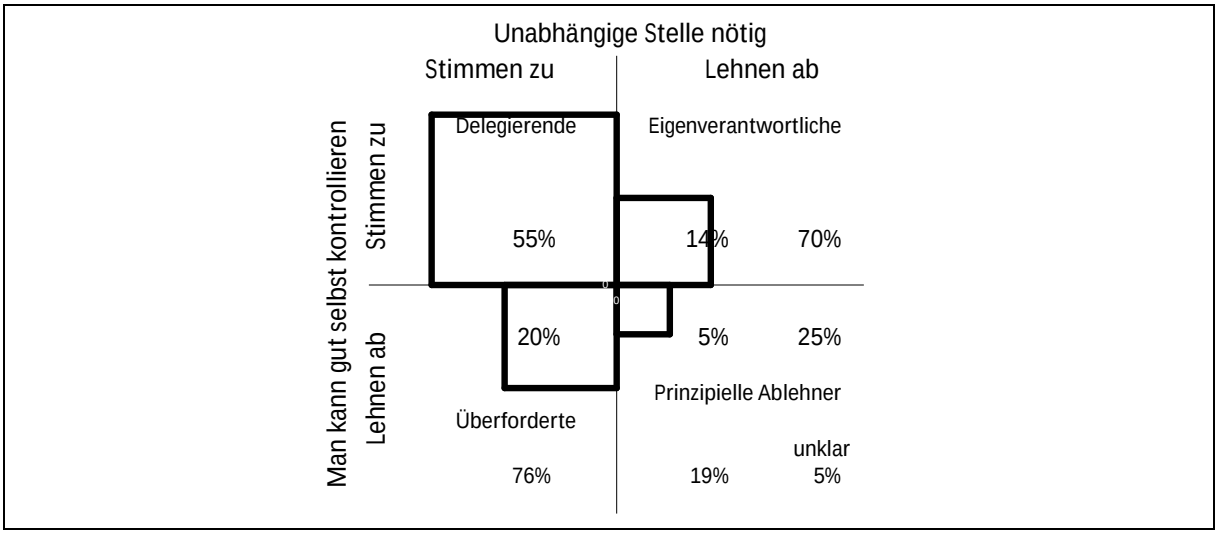


N = 1014. Der Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht"). Genaue Fragestellung vgl. Anhang 2. Beim Item „Tue soviel wie möglich..." und „Kontrolle im Internet..." wurden nur Personen befragt, die mindestens mehrmals pro Jahr das Internet nutzen (N=822).

Auch hier zeigt sich somit ein etwas ambivalentes Bild: Einerseits traut sich eine Mehrheit von mehr als zwei Dritteln der Bevölkerung zu, die Kontrolle über die persönlichen Daten zu behalten, gleichzeitig fordert eine noch grössere Mehrheit eine unabhängige Stelle, die „zum Rechten schaut".

In der Kreuztabelle (Abbildung 5-4) ist die Kombination der beiden Aussagen zur Möglichkeit des Selbstschutzes und zur Notwendigkeit einer unabhängigen Stelle dargestellt. Auch hier konnten aus den Antwortkombinationen Typen gebildet werden. Der häufigste Typus vertritt eine etwas ambivalente Haltung: 55% der Antwortenden unterstützen eine unabhängige Stelle, obwohl sie sich zutrauen, ihre Daten selbst unter Kontrolle zu halten. Denkbar ist, dass diese Personen den Schutz ihrer Daten delegieren (vgl. Label „Delegierende" in Abbildung 5-4). Eine alternative Interpretation dieses Antwortverhaltens ist, dass diese Antwortenden die unabhängige Stelle nicht für sich, sondern zum Schutz anderer Personen befürworten. Eine vertiefende Analyse dieser Gruppe anhand einer weiteren Frage lässt vermuten, dass beide Subtypen verbreitet sind: Etwas mehr als die Hälfte der Befragten dieses Typs (55%) gab an, selbst alles mögliche zu tun, um sich vor Datenmissbrauch zu schützen, rund 40% zeigten sich diesbezüglich unsicher oder gaben (selten) an, sich kaum zu schützen, obwohl sie sich das zutrauen.

Abbildung 5-4: Einstellungstypen: Selbstschutz und unabhängige Stelle



N = 1014. Genaue Fragestellung vgl. Anhang 2. Die Abweichungen in den ausgewiesenen Prozentwerten im Vergleich zu Abbildung 5-3 ergeben sich aus der höheren Anzahl Fälle mit unklaren Antworten (Kategorie „weiss nicht" bei mindestens einer der beiden berücksichtigten Fragen).

Die zweitgrösste Gruppe (20% der Antwortenden) lassen sich als Personen bezeichnen, die sich überfordert fühlen. Sie glauben nicht oder eher nicht, dass sie ihre Daten gut unter Kontrolle halten können, und erachten folgerichtig die Unterstützung durch eine unabhängige Stelle als sinnvoll. Wenig überraschend zeigt sich in dieser Gruppe nur eine Minderheit überzeugt, selbst alles Machbare zum Selbstschutz zu tun. 14% der Antwortenden halten das Prinzip der Eigenverantwortlichkeit hoch: Sie erachten sich als kompetent und eine unabhängige Stelle als unnötig; bei dieser Gruppe gibt sich eine deutliche Mehrheit überzeugt, zum Selbstschutz das Machbare auch zu tun. Beim vierten, mit 5% nur selten vertretenen Typ vermuten wir eine prinzipielle Ablehnung einer Datenschutzstelle, da diese Antwortenden den Selbstschutz zumindest nicht als einfach bezeichnet haben.

Diese insgesamt recht optimistischen Einschätzungen der Betroffenen zum Selbstschutz teilen die Interviewpartner (Experten, EDÖB) nicht. Die Sensibilität für den Schutz der Privatsphäre wird angesichts technologischen Entwicklungen zwar als eminent wichtig beschrieben, wurde aber von den befragten Experten kritisch beurteilt: Einerseits wird den Nutzerinnen und Nutzern ein geringes Interesse am Datenschutz und daran, was mit den preisgegebenen Informationen geschieht, attestiert; gerade bei jüngeren Menschen bestehe heutzutage sogar das Bedürfnis, sich im Internet darzustellen und Privates öffentlich zu machen. Die Interviewpartner vermuten, dass die Betroffenen wenig unternähmen, um den Schutz der persönlichen Daten sicherzustellen (z.B. geringe Inanspruchnahme des Auskunftsrechts, technische Massnahmen, Anpassung von Einstellungen in Sozialen Netzwerken). Andererseits verweisen sie insbesondere auch auf mangelndes Wissen über technische Möglichkeiten (z.B. Schwierigkeit, Informationen aus dem Internet zu entfernen; Datenverknüpfungen) oder über die Folgen einer Veröffentlichung privater Informationen (bspw. bei einer zukünftigen Bewerbung). Zwei Interviewpartner sprechen von einer generellen Überforderung der Benutzerinnen und Benutzer des Internet.

5.4 Haltungen zum Schutz persönlicher Angaben

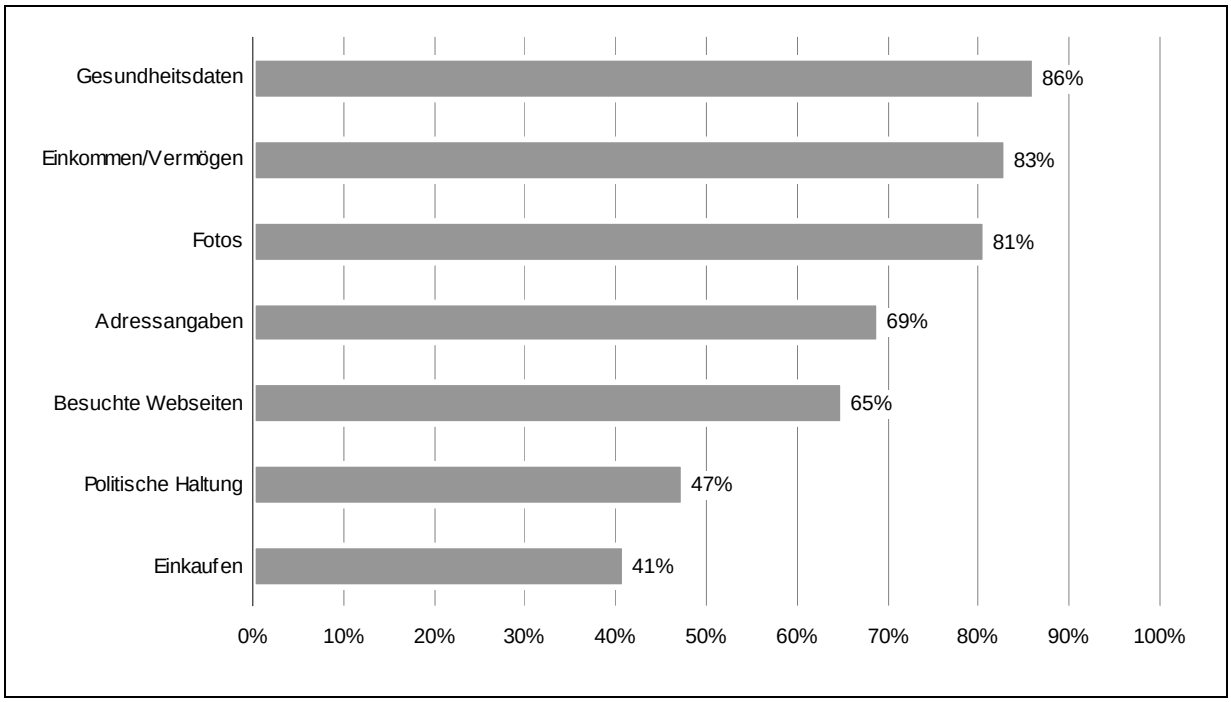
Die Umfrage von Privatim (2009) zeigte auf, dass die Bevölkerung nicht allen Daten bearbeitenden Behörden oder privaten Organisationen in gleichem Ausmass vertraut. Drei Viertel oder mehr Befragte vertrauten dieser Umfrage zufolge der Polizei, den Spitälern, den Einwohnerämtern und den Krankenkassen. Als deutlich tiefer erwies sich das Vertrauen in Kreditkartenfirmen und Telecomanbieter. Auch die Eurobarometer-Umfrage und die deutsche Umfrage zeigen ein hohes Vertrauen in medizinische Dienstleister, die Polizei und weitere Behörden sowie ein eher tiefes in einschlägige Privatfirmen wie Versandhandel oder Kreditinstitute; anders als letztere geniessen jedoch die übrigen Banken ein eher hohes Vertrauen (Eurobarometer 2008: 10; Petersen 2010).

In der vorliegenden Umfrage wurde nicht nach den Akteuren gefragt, sondern nach dem Schutzbedarf für verschiedene Arten von Daten und nach verschiedenen Praktiken von Datenbearbeitern. Auch diesbezüglich zeigen sich teils bedeutende Unterschiede in der Bevölkerung.

Eine grosse Mehrheit von 86% empfindet Angaben über die Gesundheit als (mindestens) eher schützenswert (Abbildung 5-5). Ähnlich häufig werden nur noch Daten über das Einkommen und Vermögen (83%) und Fotos der befragten Person oder ihrer Bekannten und Verwandten (81%) als schützenswert eingestuft. Rund zwei Drittel der Befragten empfinden Adressangaben (69%) und Informationen über die Webseiten, die sie besucht haben (65%) als schützenswert. Etwas weniger als die Hälfte der Befragten empfindet Angaben über die politische Haltung (47%) und über das Einkaufsverhalten (41%) als schützenswert.

Damit ergibt sich eine gewisse Diskrepanz zum DSG: Von den hier abgefragten Datenarten bezeichnet das schweizerische DSG Gesundheitsdaten sowie Daten über politische Einstellungen als besonders schützenswert. Fotos könnten zudem teilweise als Angaben über die Intimsphäre aufgefasst werden (vgl. Art. 3 Bst. c DSG). Es kann davon ausgegangen werden, dass nur eine kleine Minderheit der Befragten keine oder fast keine persönlichen Daten als schützenswert erachtet, wie eine weitere Auswertung ergab: Im Durchschnitt bezeichneten die Umfrageteilnehmerinnen und -teilnehmer 4.6 der sieben abgefragten Datenarten als schützenswert. 76% bezeichnen mindestens vier Datenarten als schützenswert, 89% bezeichneten mindestens drei Datenarten als schützenswert.

Abbildung 5-5: Einschätzung, ob persönliche Angaben schützenswert sind

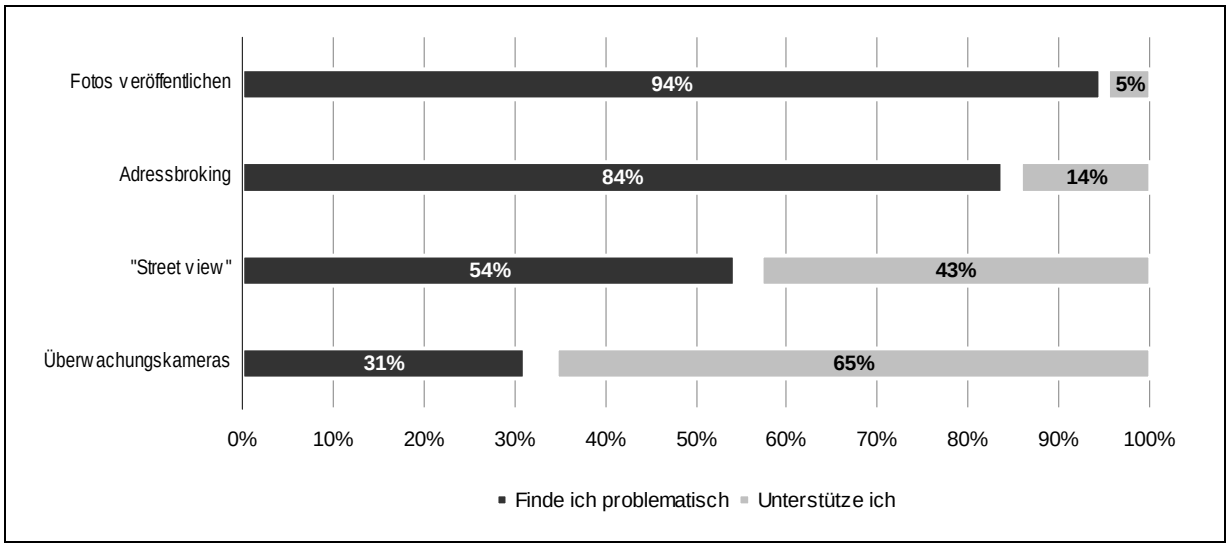


N = 1014. Genaue Fragestellung vgl. Anhang 2.

Die Befragten wurden auch zu ihrer Haltung gegenüber heute gängigen und öffentlich diskutierten Praktiken von Datenbearbeitern befragt (Abbildung 5-6). Der Umgang mit Bildmaterial der Betroffenen wird von vielen Befragten differenziert betrachtet. Die gefundenen Muster lassen sich dabei relativ gut mit Überlegungen zu den Kosten und Risiken resp. dem Nutzen der Datenbearbeitungen erklären. So beurteilen es fast alle Antwortenden (94%) als problematisch, wenn andere Leute ohne ihr Wissen Fotos veröffentlichen, auf denen sie oder Bekannte von ihnen abgebildet sind, z.B. im Internet. Was insbesondere in Sozialen Netzwerken wie z.B. Facebook potenziell häufig geschieht, scheint somit von den meisten Befragten als stossend empfunden zu werden.

Gespalten ist die Haltung der Befragten hingegen zu Anwendungen wie Google Street View: Gut die Hälfte der Befragten (54%) empfindet es als problematisch, wenn Fotos von Strassen und Plätzen im Internet veröffentlicht werden, auf denen Personen erkennbar sind. Die grössere Unterstützung dieser Art der Veröffentlichung kann daran liegen, dass die Befragten solche Bilder als weniger privat beurteilen, oder an der tiefen Wahrscheinlichkeit, dass sie selbst fotografiert werden. Zudem wird ein Teil der Befragten die angebotene Dienstleistung als nützlich empfinden.

Abbildung 5-6: Bewertung verschiedener Praktiken von Datenbearbeitern



N = 1014. Der Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht“). Genaue Fragestellung vgl. Anhang 2.

Deutlich überwiegend ist die Unterstützung mit 65% für Überwachungskameras. Der vermutete Nutzen der Datenbearbeitung, nämlich der Sicherheitsgewinn, dürfte zur hohen Zustimmung beitragen. Gleichzeitig werden wohl die Risiken als eher gering eingestuft, beispielsweise weil die Bilder im Gegensatz Facebook und Google Street View nicht veröffentlicht werden. Ebenso könnte das gegenüber privaten Unternehmen höhere Vertrauen in die Polizei (als mutmasslicher Datenbearbeiter bei der Videoüberwachung) zur positiven Beurteilung beigetragen haben.

Beim Adressbroking argumentieren die Bearbeiter mit einer Dienstleistung, die sie für die Bevölkerung erbringen. Potenziell befindet sich die Bevölkerung somit in einem Dilemma zwischen dem Schutz von Daten und einem möglichen Nutzen durch Informationen über nützliche Dienstleistungen oder Gebrauchsgüter. Von einer deutlichen Mehrheit von 84% der Befragten wird aber der Adresshandel als störend empfunden.

5.5 Einstellungen in verschiedenen soziodemographischen Gruppen

Gruppiert man die Befragten nach verschiedenen soziodemographischen Merkmalen und nach der Häufigkeit ihrer Internet-Nutzung, so zeigen sich hinsichtlich der abgefragten Einstellungen gewisse statistisch signifikante Unterschiede. Sie sind aber mit einigen Ausnahmen meist nicht markant. Errechnet wurden die Zusammenhänge anhand der Masszahl Cramer’s V (Wagschal 1999: 165). Tabelle 5-1 fasst die Resultate dieser Auswertung zusammen:

Für die Einstellungen zum Informationszeitalter spielen mehrere Merkmale eine Rolle. Männer (73%) finden den heute möglichen Informationsaustausch etwas häufiger eine gute Sache als Frauen (61%). 15-34jährige (76%) unterstützen den Informationsaustausch klar häufiger als ältere Personen – unter den 75-99jährigen stimmen der entsprechenden Aussage nur gut die Hälfte zu (53%). In der Romandie (75%) ist die Zustimmung höher als in der Deutschschweiz (65%) und

im Tessin (62%). Wenig überraschend bewerten tägliche Internetnutzer die heutigen Möglichkeiten des Inforationsaustauschs häufiger positiv (75%) als Personen, die eher selten im Internet surfen (46%).

Die Zustimmung zur Aussage, dass Datensammlungen auch beängstigend sein können, variiert nach verschiedenen Merkmalen. Männer (78%) finden Datensammlungen marginal häufiger Besorgnis erregend als Frauen (75%), Junge (15-34jährige: 82%) sorgen sich häufiger als ältere Personen (55-74jährige: 72%) und Befragte aus der Romandie (81%) und der Deutschschweiz (78%) deutlich häufiger als Befragte im Tessin (59%).

Zur Aussage „Wer nichts Unrechtes gemacht hat, dem kann es egal sein, was Andere über einem erfahren und weiterverbreiten" variiert die Zustimmung ebenfalls zwischen den Altersgruppen. Die Gruppe der 15-34jährigen stimmt am seltensten zu (33%), die Gruppe der 55-74jährigen (48%) am stärksten, was den Ergebnissen aus den Interviews widerspricht, in denen Jugendlichen eine grössere Sorglosigkeit zugesprochen wurde als älteren Personen. Ein Grund für die Diskrepanz könnte zum einen in der groben Einteilung der Alterskategorien liegen, die fallzahlbedingt gemacht werden musste; ebenfalls könnte eine Rolle spielen, dass die Unterschiede auch stark mit der Internet-Nutzung, die ebenfalls altersabhängig ist[13], zusammenhängen: Wer sich regelmässig im Internet bewegt, stimmt der Aussage deutlich seltener zu (33% bei Personen mit mehrmaliger Internetnutzung pro Woche) als Personen, die das nur selten tun (56% bei mehrmaliger Nutzung pro Jahr). Hier ist zu vermuten, dass regelmässige Internetnutzer sich ihrer Spuren sowie der Leistungsfähigkeit des Internets als Datenspeicher und für die Profilbildung viel stärker bewusst sind als seltene Nutzer. Besonders markant sind die Unterschiede zwischen den Sprachregionen: Am tiefsten ist die Zustimmung zu dieser Aussage, in der sich eine gewisse Sorglosigkeit manifestiert, in der Deutschschweiz (34%), am höchsten im Tessin mit 63%; die Romandie liegt mit 43% dazwischen. Auch die höchste absolvierte Bildungsstufe scheint schliesslich die Einstellung zu dieser Aussage zu beeinflussen: 46% der Absolventen einer Berufslehre, aber nur 26% der Hochschulabsolventen stimmen ihr zu. Die übrigen Kategorien liegen dazwischen.

Während die Einstellung zur Frage, ob man selbst kontrollieren kann, was mit den persönlichen Daten geschieht, von allen soziodemographischen Gruppen ähnlich stark bejaht wird, schwankt die Unterstützung einer unabhängigen Stelle, die „zum Rechten" zu schauen hat, etwas. Die Unterschiede sind aber nicht markant. Zwischen den Altersgruppen zeigt sich zwar ein statistisch signifikanter Zusammenhang, doch ist das Muster diffus und schwach: So ist die Unterstützung einer solchen Stelle in der Gruppe der 35-54jährigen mit 81% am höchsten, liegt aber auch in den anderen Altersgruppen über 70%. Etwas deutlicher sind die Unterschiede zwischen den Sprachregionen. Die Tessinerinnen und Tessiner befürworten eine unabhängige Stelle stärker (88%) als die Romands (72%) und die Deutschschweizer (78%). Unter den Bildungsgruppen stechen Personen mit einer Matur etwas heraus (85%), während sich die anderen Gruppen mit höherem und tieferem Bildungsniveau nahe am Bevölkerungsdurchschnitt von 78% bewegen.

Ob der Selbstschutz im Internet eher gut möglich ist oder nicht, wird in den verschiedenen Altersgruppen unterschiedlich beurteilt. Der Unterschied ist recht markant, finden doch 66% der

15-34jährigen, im Internet könne man eher gut kontrollieren, welche persönlichen Daten für andere zugänglich sind. Unter den 75-99jährigen trauen sich dies hingegen nur 40% zu. Auch vom Bildungsabschluss hängt diese Einschätzung ab, wobei das Muster nicht klar entlang den Bildungsniveaus verläuft. Von jenen Befragten, welche bloss eine obligatorische Schule abgeschlossen haben, beurteilt mit 74% der grösste Teil die Möglichkeit des Selbstschutzes als eher gut. Unter den Absolventen höherer Fachausbildungen ist der Anteil am tiefsten (54%). Dazwischen liegen Absolventen von Berufsschulen, Matura- und Seminarabsolventen sowie Hochschulabsolventen. Wie realistisch die Selbsteinschätzung der Befragten in den Gruppen jeweils ist, kann hier natürlich nicht beurteilt werden. Es sei daran erinnert, dass die befragten Experten an den Fähigkeiten der Internetnutzerinnen und -nutzer zweifeln.

Das Alter der Befragten und die Zugehörigkeit zu einer Sprachgruppe prägen somit von den hier berücksichtigten Faktoren etwaige Einstellungsunterschiede mit Bezug auf den Datenschutz am stärksten, wobei auch hier die Unterschiede häufig nicht sehr stark sind. Das Bildungsniveau, das Geschlecht und das Einkommensniveau hängen selten mit den Einstellungen zusammen.

In Bezug auf das Alter kann bilanziert werden, dass jüngere Personen dem Informationszeitalter positiver gegenüber stehen und ihre Selbstkompetenz in Bezug auf den Datenschutz etwas höher einstufen. Daraus kann aber nicht geschlossen werden, sie träten dem Informationszeitalter und den neuen Informationstechnologien sorgloser entgegen als die Angehörigen der älteren Generationen – eher ist das Gegenteil der Fall. Ähnliches lässt sich über den Vergleich regelmässiger und seltener Internetnutzer sagen, wobei Alter und Internetnutzung stark zusammenhängen. Hinsichtlich der Sprachregionen fällt vor allem auf, dass sich die Befragten der italienischen Schweiz bezüglich des Datenschutzes einerseits seltener besorgt zeigen, umgekehrt fast durchgängig eine unabhängige Stelle verlangen.

[13] 39% der befragten Personen, die das Internet seltener als mehrmals pro Jahr oder gar nie nutzen, sind älter als 74 Jahre.

Tabelle 5-1: Einstellungen nach soziodemographischen Gruppen

	Geschlecht	*Alter*	*Sprachregion*	*Schulbildung*	*Einkommen*	*Webnutzer*
„Dass man sich heutzutage mit anderen Menschen fast ständig und grenzenlos austauschen kann, ist eine gute Sache.“	0.140**	0.114**	0.083*	0.075	0.081	0.147**
„Die Vorstellung, wie viele Stellen heute Informationen über uns normale Leute sammeln und auswerten, kann einem Angst machen.“	0.084+	0.099**	0.120**	0.067	0.055	0.078
„Wer nichts Unrechtes gemacht hat, dem kann es egal sein, was Andere über einem erfahren und weiterverbreiten.“	0.017	0.105**	0.137**	0.121**	0.086	0.119**
„Mit etwas Vorsicht kann man gut selber kontrollieren, dass persönliche Informationen über einem nicht in falsche Hände geraten.“	0.044	0.061	0.051	0.087	0.085	0.050
„Es ist schwierig, unter Kontrolle zu behalten, was mit den persönlichen Angaben über einem passiert; deshalb muss eine unabhängige Stelle zum Rechten schauen.“	0.063	0.090**	0.090*	0.074	0.102*	0.071
„Glauben Sie, dass Sie sich selber so gut wie möglich vor Datenmissbrauch schützen, oder sind Sie unsicher, ob Sie diesbezüglich alles machen?“	0.060	0.110**	0.119**	0.081	0.075	0.080
„Wie ist Ihre Erfahrung, kann man im Internet als Einzelner eher gut oder eher schlecht selber bestimmen, welche Informationen über einem selbst für andere frei zugänglich sind und welche nicht?“	0.082	0.143**	0.051	0.115*	0.073	0.124**

N = 1014. Ausgewiesen wird Cramer's V. Chiquadratbasierter Signifikanztest für Gruppenunterschiede. +: Zusammenhang mit Irrtumswahrscheinlichkeit p < 10%; *:Zusammenhang mit p < 5%; **: Zusammenhang p < 1%.

Die soziodemographischen Gruppen wurden auch hinsichtlich der Art der als schützenswert eingestuften Daten global ausgewertet. In Tabelle 5-2 wird das Resultat einer Varianzanalyse ausgewiesen (vgl. Backhaus et al 2000: 70-102). Hiermit wurde untersucht, ob zwischen den einzelnen Gruppen statistisch signifikante Unterschiede bestehen hinsichtlich der durchschnittlichen Anzahl Datenarten, die als schützenswert beurteilt werden. Auch wenn die Gruppenunterschiede teilweise statistisch signifikant sind, so sind sich doch insgesamt schwach ausgeprägt.

Angehörige jüngerer Altersgruppen bezeichnen die verschiedenen Datenarten durchschnittlich leicht häufiger als schützenswert als ältere Befragte. Den Ausschlag für diesen Zusammenhang gibt vor allem die Gruppe der 75-99jährigen, die im Durchschnitt 4.1 Datenarten als schützenswert bezeichnen, während der Durchschnittswert für die anderen Gruppen um 4.6 / 4.7 liegt.

Vergleicht man allerdings die Altersgruppen hinsichtlich der einzelnen Datenarten, so ist das Bild nicht immer dasselbe. Ihre politischen Einstellungen, Angaben über das Einkaufsverhalten und Angaben über besuchte Webseiten erachten ältere Personen häufiger als schützenswert als jüngere.

Auch zwischen den Sprachregionen zeigen sich leichte Unterschiede: Dabei bezeichnen die Befragten aus dem italienischen Sprachraum im Durchschnitt 5.0 Datenarten als schützenswert, während der Durchschnitt in der übrigen Schweiz um 5.5 liegt.

Personen, deren höchste Ausbildung eine Berufslehre ist, haben im Durchschnitt eine leicht tiefere Anzahl schützenswerter Datenarten angegeben (4.4) als die übrigen Gruppen und insbesondere die Hochschulabgänger (4.9). Eine Ausnahme von diesem Muster bilden Adressangaben. Bezüglich der Internetnutzung gilt: Je häufiger eine Person das Internet nutzt, desto mehr Datenarten bezeichnet sie als schützenswert. Auch hier sind die Unterschiede jedoch klein: Wer mehrmals wöchentlich oder häufiger surft, hat im Durchschnitt 4.7 Datenarten als schützenswert bezeichnet, wer weniger als mehrmals jährlich surft, 4.3 Datenarten. Hinsichtlich der Angaben über besuchte Webseiten ist der Zusammenhang am deutlichsten: Personen, die häufig im Internet surfen, betrachten ihre Spuren etwas häufiger als schützenswert als seltene Surfer (mehrmals jährlich oder seltener).

Auch die Anzahl als problematisch eingestufter Praktiken wurde ermittelt, um hernach die Gruppen diesbezüglich zu vergleichen. Die Unterschiede sind hier noch geringer. Es zeigten sich statistisch signifikante Unterschiede nur zwischen den Geschlechtern und den Angehörigen unterschiedlicher Bildungsniveaus. Während Frauen im Durchschnitt 3.0 Praktiken als problematisch beurteilten, liegt dieser Durchschnitt bei den Männern leicht tiefer bei 2.9. Personen mit einer Berufslehre haben im Durchschnitt 2.8 Praktiken als problematisch beurteilt, während der Durchschnittswert für Hochschulabsolventen bei 3.1 liegt.

Tabelle 5-2: Schützenswerte Angaben und problematische Praktiken nach Gruppen

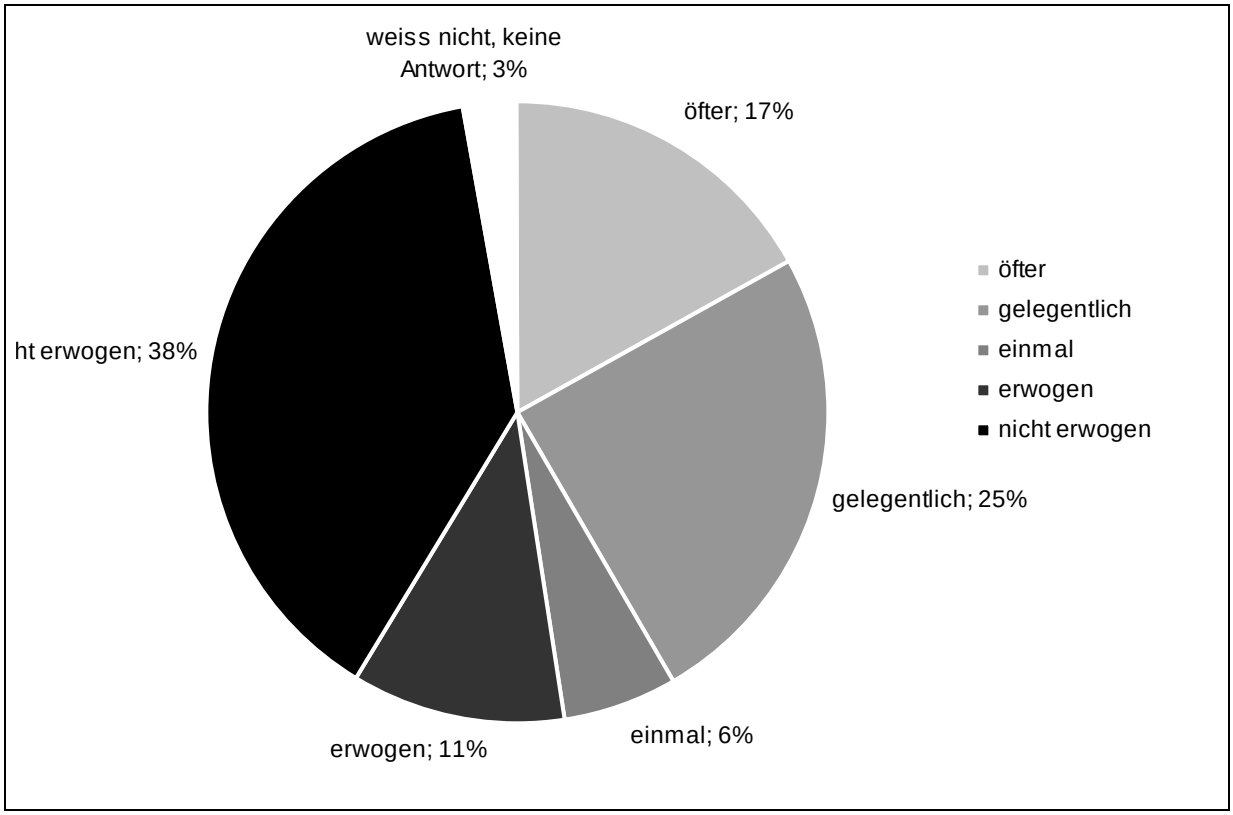
	Geschlecht	*Alter*	*Sprachregion*	*Schulbildung*	*Einkommen*	*Webnutzer*
Anzahl schützenswerte Angaben (0 bis 7) (Varianz-Analyse)	0.001	0.009+	0.009*	0.011*	0.004	0.011*
Anzahl als problematisch beurteilte Praktiken (0 bis 4) (Varianz-Analyse)	0.006*	0.004	0.001	0.010*	0.003	0.003

N = 1014. Ausgewiesen wird der Wert von R^2 der Varianzanalyse/Lineare Regression. Signifikanzangabe: F-Test fürs Gesamtmodell. +: Zusammenhang mit Irrtumswahrscheinlichkeit p < 10%: * Zusammenhang mit p < 5%; **: Zusammenhang p < 1%.

5.6 Verzicht auf kommerzielle Dienstleistung aus Datenschutzgründen

In der Umfrage gab rund die Hälfte der Personen an, schon mindestens einmal auf eine Dienstleistung verzichtet zu haben, weil zu ihrer Nutzung Angaben verlangt wurden, die man nicht zu geben bereit war. Konkret wurde gefragt: „Bei Wettbewerben, Kundenkarten oder auch anderen Dienstleistungen muss man zum Mitmachen manchmal weiter gehende Informationen über die eigene Person angeben (z.B. Geburtsdatum, Geschlecht, Beruf oder auch Hobbies). Ist es schon einmal vorgekommen, dass Sie wegen solchen Angaben auf eine Dienstleistung verzichtet haben?“ 17% der Befragten gaben an, schon öfter verzichtet zu haben, 25% gelegentlich und 6% einmal. 11% gaben an, zwar noch nie verzichtet zu haben, aber einen Verzicht aufgrund der Angaben zumindest erwogen zu haben (Abbildung 5-7).

Abbildung 5-7: Verzicht auf Dienstleistung aus Datenschutzgründen?



N = 1014; genaue Fragestellung vgl. Anhang 2.

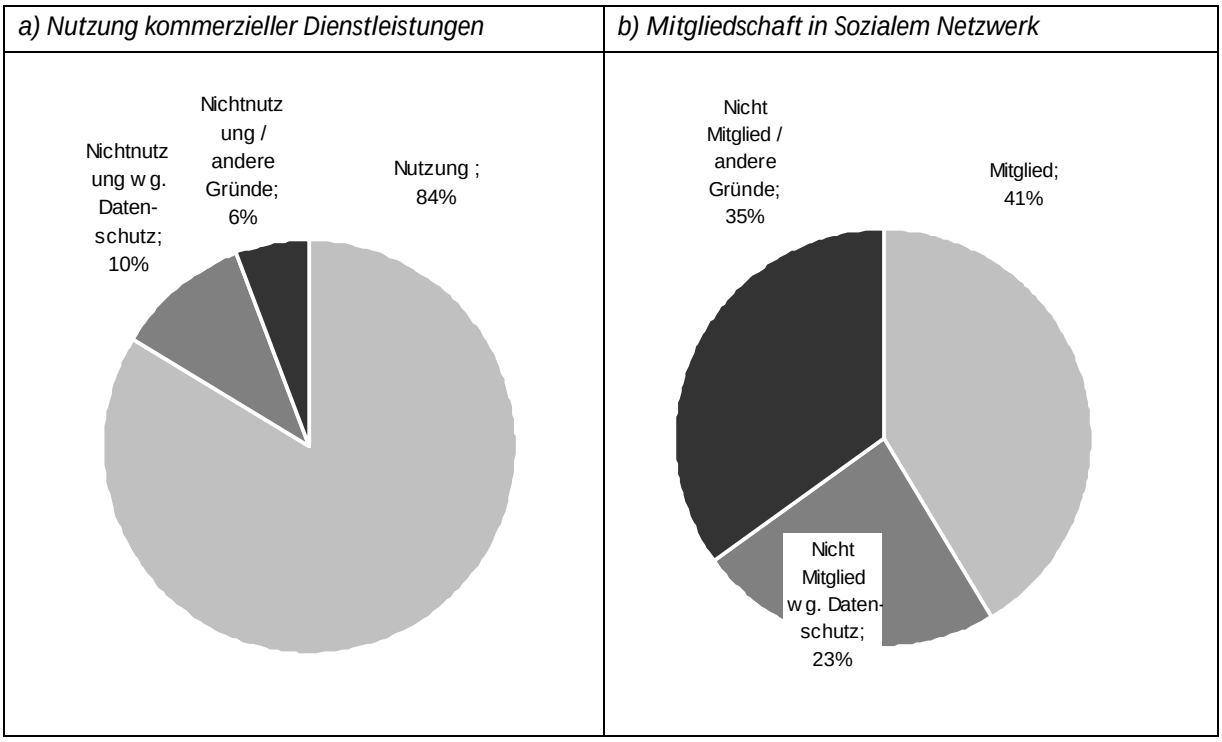
Hinsichtlich der Nutzung solcher Dienstleistungsangebote zeigen sich Unterschiede zwischen sozialen Gruppen, die allerdings nur ausnahmsweise sehr deutlich zutage treten: Männer gaben sich in der Umfrage leicht zurückhaltender als Frauen, solche Angebote zu nutzen. Personen mit dem Abschluss einer höheren Fachschule, einer Fachhochschule oder einem Universitätsabschluss sind etwas zurückhaltender als die Gruppen mit tieferen Bildungsabschlüssen. Auch bezüglich des Einkommens gibt es eine leichte Tendenz, wonach höhere Einkommensschichten eher verzichten. Deutlich ist der Unterschied, wenn man die Befragten nach ihrem Alter gruppiert. Hier fallen vorab die 75-99jährigen dadurch auf, dass bei ihnen ein Verzicht wegen persön-

lichen Angaben deutlich seltener erfolgt als bei den jüngeren Personen. Möglicherweise sind sie seltener in einer Situation, in der sie Angaben machen müssen. Auch von den Personen, die das Internet nie nutzen, verzichtet ein geringerer Anteil wegen persönlicher Angaben auf die Nutzung einer Dienstleistung. Dies erstaunt nicht sonderlich, befinden sich doch gerade in dieser Gruppe vergleichsweise viele Senioren. Alle beschriebenen Zusammenhänge sind statistisch signifikant mit einer Irrtumswahrscheinlichkeit von maximal 10% (Einkommen) respektive 5% (übrige Zusammenhänge). Zwischen den Sprachregionen zeigte sich kein verallgemeinerbarer Unterschied.

5.7 Datenschutz im Internet: Verzicht auf bestimmte Nutzungen

Die 822 Personen unter den Befragten, die mindestens mehrmals pro Jahr das Internet nutzen, wurden nach ihrer Nutzung von kommerziellen Dienstleistungen sowie nach ihrer Mitgliedschaft in Sozialen Netzwerken wie Facebook oder Xing gefragt. Bei beiden Anwendungen ist die Nutzung in der Regel mit der Bekanntgabe von persönlichen Daten verbunden. Wie Abbildung 5-8a zeigt, machten mit 84% ein Grossteil der Internetnutzer von Dienstleistungsangeboten im Internet wie etwa dem elektronischen Einkaufen, dem elektronischen Zahlungsverkehr oder dem Buchen von Reisen Gebrauch. Von den übrigen gab der grössere Teil der Befragten (insgesamt 10% aller Internetnutzer) einen Grund für die Nichtnutzung an, der zumindest teilweise mit dem Datenschutz zusammenhängen dürfte. So gaben sie etwa zu Protokoll, solche Angebote seien zu unsicher oder sie müssten zu viele persönliche Angaben machen.

Abbildung 5-8: Nutzung von und Verzicht auf Anwendungen im Internet



N = 822 Befragte. Auswahlkriterium: Internetnutzung mindestens mehrmals pro Jahr. Genaue Fragestellung vgl. Anhang 2.

Die Mitgliedschaft in Sozialen Netzwerken ist noch nicht so verbreitet wie die Nutzung kommerzieller Dienstleistungen. 41% der Internetnutzer gaben an, Mitglied in einem Sozialen Netzwerk zu sein. Unter den Nichtmitgliedern gibt zwar eine Mehrheit (insgesamt 35% der Befragten) Gründe für die Nichtteilnahme an, die mit dem Datenschutz nichts zu tun haben (Abbildung 5-8b). Dennoch verzichten 23% aller Befragten wegen Gründen, die mit dem Datenschutz in Verbindung gebracht werden können[14], auf die Nutzung Sozialer Netzwerke. Im Vergleich mit kommerziellen Dienstleistungen im Internet sind somit die grundsätzlichen datenschutzbezogenen Vorbehalte der Internetnutzer gegenüber den Sozialen Netzwerken deutlich grösser.

5.8 Vorsicht bei der Nutzung kommerzieller Dienstleistungen im Internet

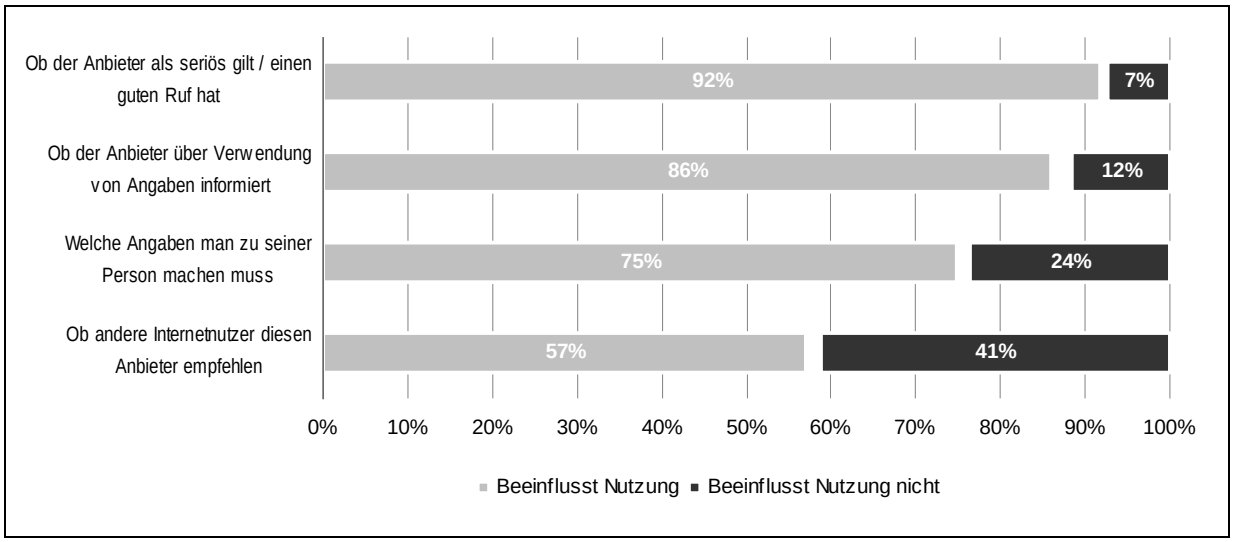
Auch wenn nur wenige Personen wegen des Datenschutzes gänzlich auf die Nutzung von Dienstleistungen im Internet verzichten, so machen die meisten Befragten die Inanspruchnahme eines Angebots im Einzelfall von verschiedenen zumindest teilweise datenschutzbezogenen Faktoren abhängig (Abbildung 5-9). So geben 92% der Nutzer an, es spiele für sie eine Rolle für den Nutzungsentscheid, ob der Anbieter als seriös gelte, respektive einen guten Ruf habe. Ebenfalls grosse Mehrheiten erachtet es als entscheidend, ob der Anbieter darüber informiert, wie er die persönlichen Angaben der Nutzer verwendet (86%) und welche persönlichen Angaben man als Nutzer machen muss (75%). Ob andere Internetnutzer einen Anbieter empfehlen, ist ebenfalls für die Mehrheit der Befragten entscheidend (57%). Wie eine weitere Auswertung ergab, geben mehr als drei Viertel der Befragten (78%) mindestens drei dieser Faktoren als entscheidungsrelevant an. Entsprechen diese Aussagen dem tatsächlichen Verhalten, so kann davon ausgegangen werden, dass die meisten Nutzer von kommerziellen Dienstleistungen wie elektronischem Einkaufen etc. im Internet sorgsam mit ihren persönlichen Angaben umgehen.

Den Eindruck, dass Dienstleistungen im Internet nicht völlig sorglos genutzt werden, vermittelt auch die deutsche Umfrage (Petersen 2010). Unterschiedlich grosse Mehrheiten der Befragten gaben in diesem Zusammenhang ihrer Furcht vor Missbrauch, Weitergabe oder Weiterverwendung ihrer persönlichen Angaben Ausdruck. Die Hälfte der Befragten gab an, sie habe schon häufiger auf Dienstleistungen im Internet verzichtet, weil sie ihre Daten nicht preisgeben wollten. Nur eine kleine Minderheit der Befragten gab an, die Preisgabe der Daten sei unbedenklich oder sogar nützlich.

Die durchschnittliche Anzahl der von den Befragten als entscheidungsrelevant bezeichneten Kriterien unterscheidet sich in den verschiedenen Altersgruppen und in den Sprachregionen statistisch signifikant. Jüngere Personen wenden durchschnittlich mehr Kriterien an als ältere, die Bewohner der Romandie und der Deutschschweiz mehr als die Bewohner des Tessins. Die Irrtumswahrscheinlichkeit liegt in beiden Fällen unter 5%. Die Häufigkeit, mit der Personen das Internet nutzen, hängt wie die übrigen soziodemographischen Merkmale nicht mit der Anzahl entscheidungsrelevanter Kriterien bei der Inanspruchnahme von Internet-Dienstleistungen zusammen.

[14] Dazu wurden folgende Begründungen gezählt: „Ich finde das zu unsicher"; „Ich muss zuviel persönliche Angaben machen" (vgl. Fragebogen Anhang 2).

Abbildung 5-9: Kriterien bei der Nutzung einer Internet-Dienstleistung



N = 688 Nutzer von kommerziellen Dienstleistungen im Internet. Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht“). Genaue Fragestellung vgl. Anhang 2.

5.9 Risikobewusstsein in Sozialen Netzwerken

Auch die Mitglieder Sozialer Netzwerke (351 Befragte) wurden mit zusätzlichen Aussagen zu datenschutzrelevanten Fragen im Zusammenhang mit diesen Netzwerken befragt. Allerdings wurden hier eher Einstellungen als das konkrete Verhalten abgefragt. Die Befragten signalisierten insgesamt ein grosses Bewusstsein für die Datenschutzrisiken im Internet. 94% stimmten der Aussage zu, dass die Leute im Sozialen Netzwerk oft zuwenig darüber nachdenken, welche persönlichen Angaben sie dort bekannt geben. Dass im Sozialen Netzwerk die ausgetauschten Informationen harmlos sind, glaubt nur eine Minderheit von 18% der Antwortenden (Abbildung 5-10).

Gleichzeitig neigen 86% zur Ansicht, dass es in Sozialen Netzwerken einfach sei, die Benutzung so einzustellen, dass man den Personenkreis, dem man seine Daten bekannt gibt, unter Kontrolle halten kann. Ob alle zustimmenden Befragten die Einstellungen tatsächlich entsprechend verändern, ist jedoch zu bezweifeln. Aussagen von Facebook-Chef Mark Zuckerberg zufolge hat nur die Hälfte der Mitglieder seines Netzwerks die Einstellungen je verändert (Basler Zeitung online vom 3.6.2010). In eine ähnliche Richtung deuten auch die Antworten auf die – allerdings nicht internetspezifisch formulierte – Frage der vorliegenden Umfrage, ob man den Eindruck habe, man tue alles Mögliche, um sich vor Datenmissbruch zu schützen: Von den 86%, welche die Kontrolle im Sozialen Netzwerk als einfach beurteilen, zweifelt knapp die Hälfte der Befragten daran, dass sie alles Mögliche zum Selbstschutz täten oder gibt sogar an, man schütze seine persönlichen Daten nicht.

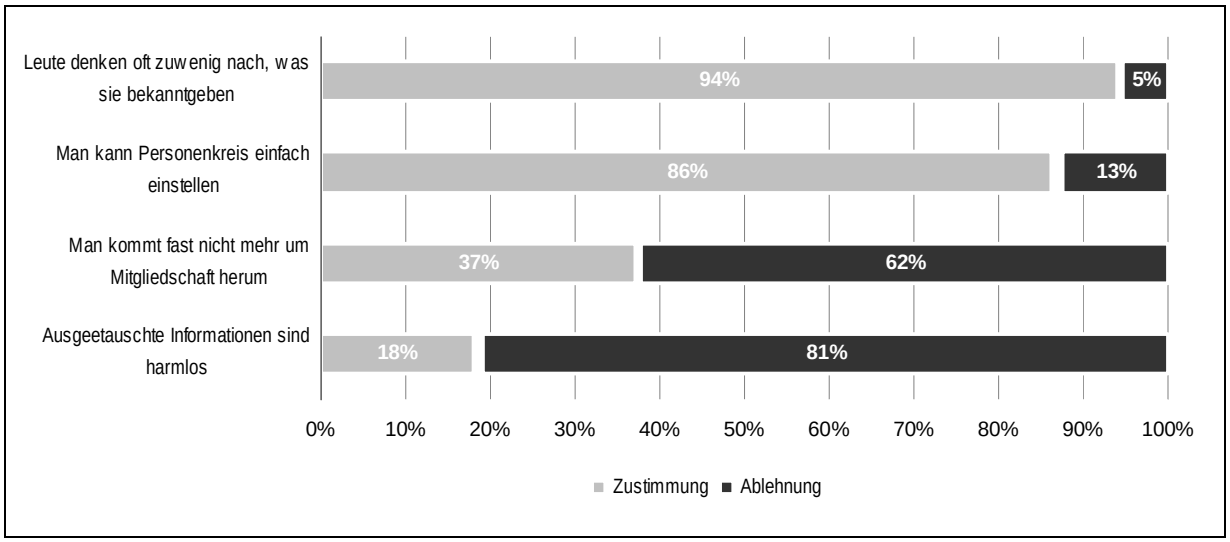
Ebenfalls kritisch beurteilten die Experten und die Mitarbeitenden des EDÖB in den Interviews das Selbstschutzverhalten der Mitglieder in Sozialen Netzwerken. Dies erstaunt nicht angesichts der Tatsache, dass die Interviewpartner wie beschrieben bei einem grossen Teil der Bevölkerung

eine geringe Sensibilität für den Datenschutz vermuten. Dabei ist ihnen zufolge nicht nur zu beachten, wie mit den eigenen Daten umgegangen wird, sondern auch das Problem zu gewärtigen, dass durch die Veröffentlichung von Bildern und Videos auch die Privatsphäre Dritter verletzt werden kann. Insgesamt attestieren die Interviewpartner den Privatpersonen im Umgang mit verschiedenen Angeboten im Internet (Soziale Netzwerke, aber auch Twitter, Youtube, Online-Bestellungen, Smartphone) ein ungenügendes Bewusstsein um datenschutzrelevante Aspekte.

Sozialen Druck, einem Netzwerk beizutreten, verspürt von den Befragten nur eine – allerdings bedeutsame – Minderheit. Darauf weist die Zustimmung von 37% zur Aussage „Heutzutage kommt man fast nicht mehr darum herum, sich in solchen Netzwerken zu bewegen“ hin.

Aus der Kombination der Einstellungen zu Sozialen Netzwerken konnte ein Index gebildet werden, der näherungsweise erfasst, mit wie grossen Vorbehalten die Befragten den Netzwerken begegnen. Als je ein Vorbehalt wurde die Zustimmung zur Aussage „Leute denken zuwenig nach“ sowie die Ablehnung zu den Aussagen „Man kann den Personenkreis einfach bestimmen“ und „Ausgetauschte Informationen sind harmlos“ gewertet werden. Insgesamt konnten die Befragten somit null bis drei Vorbehalte anmelden. Im Durchschnitt betrug die Anzahl Vorbehalte 1.9. Der Vergleich verschiedener sozialer Gruppen ist aufgrund der geringen Fallzahl von 351 Netzwerkmitgliedern unter den Befragten nur zurückhaltend zu interpretieren. Tendenziell gilt, dass jüngere Personen sich vorsichtiger äussern als ältere, Romands und Deutschschweizer vorsichtiger als Tessiner sowie häufige Internetnutzer vorsichtiger als eher seltene Internetnutzer.

Abbildung 5-10: Einstellungen zu Risiken in Sozialen Netzwerken



N = 351 Mitglieder eines Sozialen Netzwerks. Der Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht“). Genaue Fragestellung vgl. Anhang 2.

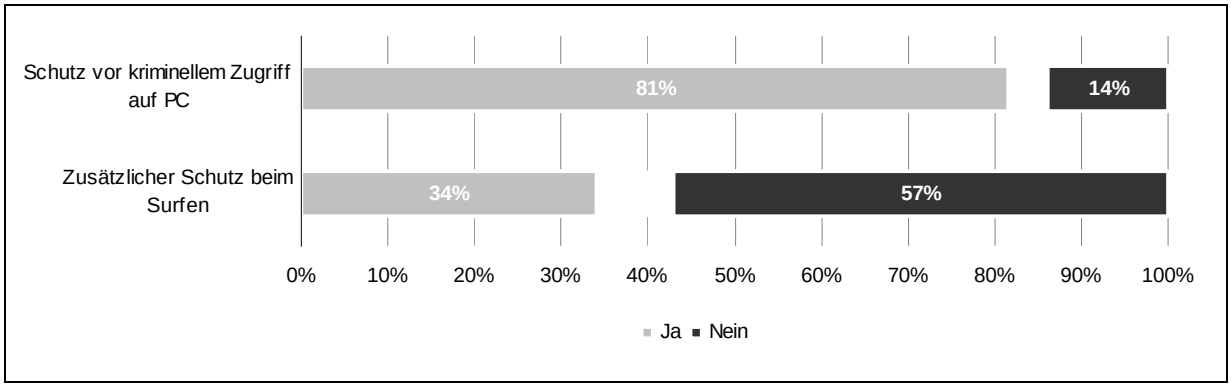
5.10 Datensicherheit am eigenen Computer und im Internet

Eine grosse Mehrheit von 81% der 822 befragten Internetnutzerinnen und -nutzer hat auf dem Computer technische Vorkehrungen (wie Virenschutzprogramme, Firewall, Cookiefilter) getroffen, die ihn/sie vor unerlaubten Zugriffen auf persönliche Daten schützen sollen. Von einem

darüber hinausgehenden Schutz, der das Hinterlassen von Spuren im Internet eindämmen soll, etwa durch eine Verschlüsselung von Suchbefehlen und E-Mails oder durch anonymisiertes Surfen, berichten 34% der Internetnutzer (Abbildung 5-11).

Führt man die beiden Fragen zusammen, so zeigt es sich, dass 16% der Befragten keine der beiden Schutzstrategien anwenden und 31% beide Schutztypen. 53% wenden einen Schutztyp (meist Virenschutz/Firewall/Cookiefilter) an. Hinsichtlich des installierten Schutzes zeigen sich auch gewisse Unterschiede zwischen den sozialen Gruppen. Während das Geschlecht und das Alter nicht ausschlaggebend sind, zeigt sich ein sprachregionales Muster: So verneinen mit 34% mehr als ein Drittel der Befragten aus dem Tessin, sich zu schützen, während dies in der Deutschschweiz 23% und in der Romandie 11% einräumen. Weiter steigt das Niveau des technischen Datenschutzes auf dem eigenen PC mit dem Bildungsniveau und dem Einkommen an, wobei Hochschulabgänger als Ausnahme von dieser Regel im Durchschnitt nur ein mittelmässiges Niveau aufweisen. Wer häufig im Internet ist, verfügt tendenziell auch über ein etwas höheres Schutzniveau als Personen, die nur selten surfen.

Abbildung 5-11: Technische Schutzvorkehrungen



N = 822 Internetnutzer. Der Abstand zwischen grauen und schwarzen Balken veranschaulicht die fehlenden Prozent bis 100% (Kategorie „weiss nicht"). Genaue Fragestellung vgl. Anhang 2.

6 Zusammenfassung und Fazit zum Umfeld des DSG

Die drei Kapitel des zweiten Teils dieser Evaluation zeigen eine Auslegeordnung der technologischen Entwicklungen sowie der Sensibilität der Datenbearbeiter und der Bevölkerung für den Datenschutz. Letztere bilden die Rahmenbedingungen, innerhalb derer sich die Wirkungsmechanismen des DSG, die Gegenstand der beiden folgenden Teile III und IV dieser Untersuchung sein werden, entfalten können resp. an ihre Grenzen stossen.

6.1 Technologische Entwicklungen

Die technologischen Entwicklungen seit Inkrafttreten des DSG 1993 haben dazu geführt, dass die Menge an Informationen an sich, die Zahl der Geräte und Anwendungen, welche Daten produzieren, und die Möglichkeiten, wie diese Informationen erhoben, gespeichert und ausgewertet werden können, massiv zugenommen haben. Der Mensch hinterlässt in den unterschiedlichsten Lebensbereichen bewusst oder unbewusst Spuren; insbesondere das Internet mit unterschiedlichsten Anwendungen, bei denen Personendaten bearbeitet werden, bringt neue Herausforderungen mit sich. Zudem gewinnt die internationale Dimension von Datenbearbeitungen immer mehr an Bedeutung. Diese Entwicklungen fordern die Datenbearbeiter, die betroffenen Personen und die mit dem Vollzug des DSG betrauten Akteure heraus, denn sie führen teilweise zu komplexen, intransparenten Situationen: Die Zahl der Beteiligten nimmt zu, der Zweck und der Kontext der Datenbearbeitung vervielfältigt sich, die Datenbearbeitung erfolgt zum Teil durch Techniksysteme spontan und grenzübergreifend, und die Wirkungen dieser Bearbeitungen sind nur schwer abzuschätzen. Für die Betroffenen wird es immer schwieriger, einen Überblick über die persönlichen Daten, die von Dritten bearbeitet werden, zu behalten. Auch die Durchsetzung der gesetzlichen Vorschriften wird angesichts dieser immer häufiger, immer unübersichtlicher und internationalisierter erfolgenden Datenbearbeitungen potenziell erschwert. Die Entwicklung hat zwar auch datenschutzfreundliche Technologien hervorgebracht, doch deren Verbreitung hält mit der Zunahme der Datenbearbeitungen nicht Schritt. Festzuhalten bleibt, dass neben diesen neuen, unübersichtlichen Konstellationen die eher klassischen Datenbearbeitungen mit klar ersichtlichem Bearbeiter und mehr oder minder transparenten Bearbeitungen weiterhin vorhanden sind und mengenmässig ebenfalls zugenommen haben.

6.2 Sensibilität der Datenbearbeiter

Die Sensibilität der privaten und öffentlichen Datenbearbeiter für den Datenschutz sowie deren Handhabung datenschutzrechtlicher Bestimmungen waren Gegenstand von Kapitel 4. Dabei hat sich gezeigt, dass das Risiko für die Datenbearbeiter, aufgrund der Durchsetzungsmechanismen des DSG (vgl. dazu im Folgenden Teil III und IV) sanktioniert zu werden, ebenso wie die Schwere möglicher Sanktionen, als gering einzustufen sind. Die beschriebenen technologischen Entwicklungen bieten ein wirtschaftliches Potenzial für gewinnorientierte Firmen, und auch im staatlichen Bereich eröffnen sich neue Möglichkeiten, beispielsweise bei der Überwachung und Fahndung nach bestimmten Personen, im Bereich der Statistik oder beim Austausch zwischen

verschiedenen Behörden zum Verhindern von Leistungsmissbrauch (Bolliger/Féraud 2010). Daneben finden sich in beiden Bereichen auch Anreize zu einem gesetzeskonformen Verhalten: In der Privatwirtschaft müssen Unternehmen vor allem einen drohenden Imageschaden im Falle einer Rechtsverletzung, die öffentliches Aufsehen erregen könnte, mitberücksichtigen. Das Einhalten der Grundsätze des DSG ist für das Vertrauen der Kundschaft in eine Unternehmung von Bedeutung. Daneben besteht für private Bearbeiter auch das Risiko, dass Produkte und Dienstleistungen verboten werden und damit getätigte Investitionen verloren gehen. Bundesbehörden betonen demgegenüber die Bedeutung eines intakten Vertrauensverhältnisses zwischen dem Bürger und dem Staat; ausserdem setzt das Legalitätsprinzip den öffentlich-rechtlichen Datenbearbeitern wirksame Schranken und sorgt für Transparenz über bestehende und geplante Bearbeitungen.

Insgesamt kann aufgrund der vorliegenden empirischen Evidenz bilanziert werden, dass eine grosse Mehrheit der Datenbearbeiter, die in der Schweiz ansässig sind, einigermassen sensibilisiert ist und die Bestimmungen des DSG anwendet, wenn auch in pragmatischer Art und Weise. Gleichzeitig bestehen deutliche Unterschiede: So wurde in den Interviews mit Experten beispielsweise vermutet, dass grosse Firmen – wegen ihrer Bekanntheit und dem damit verbundenen potenziell schweren Imageschaden im Falle eines Verstosses gegen das Gesetz – stärker darum bemüht sind, sich regelkonform zu verhalten. Demgegenüber besitzen kleinere und mittlere Unternehmen in der Regel über keine professionellen Strukturen im Datenschutzbereich, es sei denn, der Umgang mit Personendaten gehöre zu ihrem Kerngeschäft. Bei Bundesbehörden wird teilweise eine bessere Beachtung der Datenschutzbestimmungen vermutet.

Hinweise auf die Einhaltung des DSG durch die Datenbearbeiter lassen sich darüber hinaus aus anderen empirischen Erkenntnissen dieser Evaluation ziehen: So gab im Rahmen der Bevölkerungsumfrage rund ein Fünftel der Befragten an, schon einmal von einem Missbrauch ihrer persönlichen Daten betroffen gewesen zu sein (vgl. Ziffer 8.2.1). Auch im Rahmen der Fallstudien und der Analyse der Aktivitäten des EDÖB zeigt sich, dass es in der Praxis zu Datenschutzverletzungen kommt (vgl. Kapitel 12). Die Analyse der Rechtsprechung zeigt, dass es jedoch selten zu Gerichtsfällen kommt. Somit lässt sich bilanzieren, dass die Datenschutzbestimmungen in der Praxis nicht immer eingehalten, sondern mit einem gewissen Pragmatismus umgesetzt werden. Schwerwiegende Missbrauchsfälle sind wenige bekannt; vermutlich besteht aber eine Dunkelziffer.

6.3 Sensibilität der betroffenen Personen

Die Ergebnisse der Bevölkerungsbefragung erlauben es, die Sensibilität der betroffenen Personen zu beurteilen. Eine Mehrheit der Befragten begrüsst die entstandenen Möglichkeiten der Informationsgesellschaft. Gleichzeitig wird der Datenschutz von einer Mehrzahl als wichtig erachtet, wobei die Ergebnisse eine differenzierte Haltung zeigen: Der Datenschutz wird je nach Art der Daten sowie nach der Art der Bearbeitung als unterschiedlich wichtig beurteilt. Nur eine kleine Gruppe der Befragten kann als sorglos im Umgang mit ihrer Privatsphäre in dem Sinne bezeichnet werden, dass sie dem Schutz der Daten ungeachtet ihrer Beschaffenheit und der Art der Bearbeitung eine tiefe Relevanz beimisst.

Eine grosse Mehrheit der Befragten ist der Meinung, dass ein ausreichender Selbstschutz vor Datenmissbrauch durchaus möglich ist, wobei wiederum ein bedeutender Anteil in dieser Gruppe einräumt, sich diesbezüglich nicht immer konsequent zu verhalten. Mehr als drei Viertel unterstützen auch die Aussage, dass es eine unabhängige Stelle braucht, welche für die Einhaltung des Datenschutzes sorgt. Die befragten Experten beurteilen die Möglichkeit, den Überblick über Datenbearbeitungen zu gewinnen, aufgrund der Vielzahl der bewusst oder unbewusst erfolgten Bearbeitungen von persönlichen Daten als praktisch unmöglich; ebenfalls attestieren sie den Betroffenen diesbezüglich ein geringeres Interesse und tiefere Kenntnisse von Bearbeitungsmöglichkeiten als dies in deren Selbsteinschätzung im Rahmen der Bevölkerungsbefragung zum Ausdruck kommt. Dies weist darauf hin, dass die Betroffenen die aktuellen Möglichkeiten der Datenbearbeitung möglicherweise unterschätzen.

Ein ambivalentes Bild, das zu diesem Befund passt, ergibt die Bevölkerungsumfrage in Bezug auf verschiedene konkrete Situationen, bei denen persönliche Daten im Spiel sind. Eine Mehrheit der Personen, die das Internet nutzen, beansprucht kommerzielle Dienstleistungen. Überlegungen zum Datenschutz sind dabei für eine Mehrheit der Befragten ein Thema, jedoch selten ein Grund, um tatsächlich auf die Inanspruchnahme einer Dienstleistung zu verzichten; eine kleine Minderheit verzichtet aus Datenschutzüberlegungen vollständig auf solche Angebote. Ebenfalls ein beträchtlicher Teil der Internetnutzer (rund 40%) sind Mitglied in einem Sozialen Netzwerk; etwas mehr als 20% der Internetnutzer geben an, dass (auch) der Datenschutz ein Grund für die Nicht-Mitgliedschaft sei. Zwar lässt die Umfrage darauf schliessen, dass sich die meisten Mitglieder von Sozialen Netzwerken durchaus mit datenschutzrechtlichen Fragen auseinandersetzen und diese Austauschplattformen nicht als völlig unbedenklich einschätzen. Andere Ergebnisse der Befragung sowie die Einschätzungen von Experten führen jedoch zu einer kritischeren Beurteilung der Frage, inwiefern sich die Mitglieder von Sozialen Netzwerken ausreichend schützen. Technische Sicherheitsmassnahmen werden von einer Mehrheit verwendet, allerdings geht der technische Datenschutz in der Mehrheit der Fälle nicht sehr weit. Immerhin 16% der Befragten treffen keine technischen Vorkehrungen wie die Installation eines Virenschutzprogramms, von Firewalls oder einem Cookiefilter – oder sie wissen nicht, dass diese auf ihrem Computer installiert sind.

Insgesamt ergibt sich aus der Befragung somit das Bild einer Bevölkerung, welche in der Mehrheit ein Interesse am Schutz ihrer persönlichen Daten besitzt, und Schattenseiten der neuen Möglichkeiten des Informationsaustauschs in Bezug auf die Wahrung der Privatsphäre durchaus wahrnimmt. Bei eher konventionellen Anwendungen wie der Nutzung einer Dienstleistung – sei es im Internet oder nicht – spielt der Datenschutz für eine grosse Bevölkerungsgruppe eine Rolle. Bezüglich neueren Möglichkeiten des Internet wie z.B. Sozialen Netzwerken, ist es fraglicher, ob von den Nutzerinnen und Nutzern das prinzipiell breit verankerte Datenschutzbewusstsein auch in entsprechendes Verhalten umgemünzt wird. Für die Antwort auf die Frage, inwiefern die Betroffenen selber dazu in der Lage sind, den Überblick über ihre persönlichen Daten zu behalten und sich selber zu schützen, liefert die Befragung keine deutlichen Muster; skeptisch beurteilen die befragten Experten diesen Punkt. Viele Befragte selbst sind hinsichtlich des Ausmasses ihres Selbstschutzes durchaus selbstkritisch.

6.4 Gesamtbilanz

Bilanzierend lässt sich somit mit Blick auf die Wirksamkeit der Durchsetzungsmechanismen des Datenschutzgesetzes, die in den beiden folgenden Teilen näher analysiert werden, festhalten, dass sowohl bei den Datenbearbeitern als auch bei den Betroffenen nicht von einer umfassenden Sensibilität ausgegangen werden kann. Während wir nicht annehmen können, dass die Bestimmungen des DSG von den Bearbeitern flächendeckend umgesetzt werden, hat der Datenschutz für die Betroffenen zwar mehrheitlich ein hohes Gewicht, Kenntnisse über bestimmte Bearbeitungsformen oder die getroffenen Massnahmen zum Selbstschutz entsprechen dem aber nur teilweise. Erschwerend kommt hinzu, dass sich angesichts der rasanten und schwer abschätzbaren technologischen Entwicklungen laufend neue Herausforderungen in Bezug auf beide Akteursgruppen ergeben: Datenbearbeiter haben immer weiter gehende Möglichkeiten, Personendaten zu bearbeiten, und auch beträchtliche ökonomische Anreize, diesen Spielraum auszunutzen; die Betroffenen sehen sich demgegenüber nicht mehr nur mit Datenbearbeitungen im klassischen Sinn konfrontiert, sondern vermehrt mit Konstellationen, die hinsichtlich des Selbstschutzes hohe Anforderungen an die Betroffenen stellen, weil einmal preisgegebene Daten viel schneller und intransparenter weitergegeben und verbreitet werden können, und weil dabei nationale Grenzen oft kein Hindernis mehr darstellen.

TEIL III: WIRKUNGSMECHANISMUS DER DURCHSETZUNGSRECHTE

Nachdem sich Teil II der Evaluation mit dem Kontext sowie mit der Sensibilität der Datenbearbeiter und der Betroffenen befasst hat, wendet sich die Evaluation in diesem und im folgenden Teil den beiden Wirkungsmechanismen des DSG zu (vgl. Wirkungsmodell Ziffer 2.2). Im Zentrum dieses Teils der Evaluation stehen die Betroffenen selber: Das DSG gibt ihnen Instrumente in die Hand, mit denen sie Persönlichkeitsverletzungen durch private oder öffentliche Datenbearbeiter auf dem Gerichtsweg geltend machen können. Die Wirksamkeit dieser Rechte soll im Folgenden näher untersucht werden; es wird insbesondere zu prüfen sein, inwiefern die Bestimmungen des DSG geeignet sind, den Schutz von Personendaten angemessen zu gewährleisten. Mit der Wirksamkeit des Aufsichtsorgans wird sich daran anschliessend Teil IV näher befassen.

Kapitel 7 stellt die massgeblichen gesetzlichen Grundlagen zu den Durchsetzungsrechten der Betroffenen vor und vergleicht diese mit den Bestimmungen in anderen Ländern. Kapitel 8 nimmt den für die Wirksamkeit der verschiedenen Durchsetzungsrechte zentralen Begriff der Sensibilität der betroffenen Personen wieder auf. Ergänzend zu den bereits im Teil II diskutierten Befunden zu den Einstellungen und Aspekten des Verhaltens der Bevölkerung wird die empirische Evidenz zu den Kenntnissen des DSG bei den Betroffenen und dem Verhalten in Missbrauchssituationen präsentiert. Vor diesem Hintergrund wird die tatsächliche Inanspruchnahme der Durchsetzungsrechte der Betroffenen quantitativ festgehalten und eingeordnet.

Kapitel 9 umfasst eine Darstellung und Analyse von Gerichtsurteilen. Von Interesse ist im Besonderen, wie die DSG-Bestimmungen von den Gerichten angewendet und konkretisiert werden. Kapitel 10 fasst schliesslich die gewonnenen politologischen und juristischen Erkenntnisse zusammen.

7 Gesetzliche Bestimmungen im internationalen Vergleich

In diesem Kapitel werden das Einsichtsrecht (Art. 8 DSG) sowie die Durchsetzungsrechte nach Art. 15 und Art. 25 DSG, welche das DSG den Betroffenen zur Verfügung stellt, kurz vorgestellt. Dabei wird nach Bearbeitungen von Personendaten durch Private und Bundesorgane unterschieden. Ebenfalls werden die vorhandenen Instrumente mit Hilfe des internationalen Vergleichs eingeordnet. Dabei stützen wir uns einerseits auf die vorhandene juristische Literatur zum Datenschutzgesetz, andererseits wird für den internationalen Vergleich die Studie des SIR (2010) herangezogen.

7.1 Bearbeitung durch Private

Die Datenbearbeitung durch Private darf gemäss Art. 12 Abs. 1 DSG nicht widerrechtlich sein. Damit knüpft das DSG direkt an den Persönlichkeitsschutz nach Art. 28 ZGB an: Eine Verletzung der Persönlichkeit liegt vor, wenn Daten entgegen den Grundsätzen der Datenbearbeitung bearbeitet werden, wenn Daten einer Person gegen deren ausdrücklichen Willen ohne Rechtfertigungsgrund bearbeitet werden, oder wenn besonders schützenswerte Daten ohne Rechtfertigungsgrund bekannt gegeben werden. Die Bearbeitung ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 13 Abs. 1 DSG). Art. 13 Abs. 3 konkretisiert, unter welchen Bedingungen insbesondere ein überwiegendes Interesse der bearbeitenden Person im Vergleich zum Schutzinteresse der betroffenen Person in Betracht kommt.

Eine betroffene Person kann gegen die Verletzung des Persönlichkeitsschutzes vor einem Zivilgericht Klage erheben oder eine vorsorgliche Massnahme beantragen (Art. 15 DSG). Sie kann verlangen, dass die Bekanntgabe an Dritte gesperrt wird, dass die Daten berichtigt werden, dass sie vernichtet werden, oder dass bei Unklarheit über die Richtigkeit ein entsprechender Vermerk über die Bestreitung der Richtigkeit angebracht wird. De facto führt letzteres zu einer Umkehr der Beweislast bei der Frage der Richtigkeit von Daten (Maurer-Lambrou/Vogt 2006: 220). Die betroffene Person kann auch verlangen, dass eine Berichtigung, eine Vernichtung, eine Sperre, ein Vermerk oder das Gerichtsurteil Dritten mitgeteilt oder veröffentlicht wird. Auch ihr Auskunftsrecht nach Art. 8 DSG kann die betroffene Person gerichtlich durchsetzen. Das Verfahren richtet sich nach dem ZGB (Art. 28 bis Art. 28l ZGB).

Auf Antrag der betroffenen Person können private Datenbearbeiter mit Busse (bis 10'000 CHF vgl. Rosenthal/Jöhri 2008: 681) bestraft werden, wenn sie vorsätzlich ihre Informations- und Auskunftspflichten (die in den Artikeln 7a bis 10 niedergelegt sind) verletzen (Art. 34 Abs. 1 DSG). Eine Verletzung kann dabei im Unterlassen einer Information oder in der Erteilung falscher oder unvollständiger Auskünfte liegen.

7.2 Bearbeitung durch Bundesorgane

Bundesorgane dürfen Personendaten nur dann bearbeiten (und damit in die informationelle Selbstbestimmung der betroffenen Person eingreifen), wenn dafür eine gesetzliche Grundlage besteht (Art. 17 Abs. 1 DSG). Für besonders schützenswerte Personendaten und Persönlichkeitsprofile ist (mit gesetzlich umschriebenen Ausnahmen) ein Gesetz im formellen Sinn erforderlich (Art. 17 Abs. 2 DSG). Das generell für staatliches Handeln geltende Legalitätsprinzip findet sich somit auch im Datenschutzbereich und setzt damit der Datenbearbeitung engere Grenzen als die Bestimmungen im privatrechtlichen Teil (Rosenthal/Jöhri 2008: 457). Im Weiteren gibt das Gesetz den Bundesorganen Handlungsanweisungen für bestimmte Bearbeitungsformen (Beschaffen, Bekanntgabe, Anonymisieren und Vernichten).

Wer ein schutzwürdiges Interesse hat, kann sich gegen widerrechtliche Bearbeitungen durch ein Bundesorgan wehren (Art. 25 DSG). Die Rechte sind dabei dieselben wie bei der Bearbeitung durch Private. Auch gegenüber Bundesorganen kann die Auskunft nach Art. 8 DSG verlangt werden.

Für die Durchsetzung ihrer Rechte müssen die Betroffenen ein Gesuch beim Bundesorgan einreichen, worauf sie eine anfechtbare Verfügung erhalten. Beschwerden können sie nach Durchlaufen der verwaltungsinternen Einsprache- und Beschwerdeinstanzen an das Bundesverwaltungsgericht (BVerwG) richten.[15] Der Entscheid des Bundesverwaltungsgerichts kann mit Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht weitergezogen werden (der Rechtsschutz richtet sich nach den allgemeinen Bestimmungen der Bundesrechtspflege; Art. 33 Abs. 1 DSG).

Die gerichtlich durchsetzbaren Rechte der Betroffenen sind somit gegenüber den Bundesorganen grundsätzlich dieselben wie gegenüber einem privaten Datenbearbeiter. Anders sind der einzuschlagende Beschwerdeweg und aufgrund des Legalitätsprinzips auch das Prüfprogramm bei der Fallbeurteilung.

7.3 Die Rechtsdurchsetzung im internationalen Vergleich

Bezüglich der Durchsetzungsrechte hat die EG-Richtlinie 95/46 zu einer Harmonisierung geführt, verlangt doch deren Art. 12 Bst. b, dass die Mitgliedstaaten das Recht auf Berichtigung, Löschung und Sperrung gewährleisten.

Alle berücksichtigten Staaten haben denn auch zur Durchsetzung des Datenschutzrechts für die Betroffenen Rechtsansprüche festgelegt (Tabelle 7-1). Gegenüber *privaten Datenbearbeitern* bestehen die Rechte auf Auskunft, auf Vernichtung, Berichtigung und Sperrung in allen im Rechtsvergleich berücksichtigten Staaten. Ein Vermerkrecht analog zur Schweiz fehlt hingegen häufig. Kanada, Grossbritannien und Slowenien kennen ein solches teilweise. Auch in Deutschland fehlt das Vermerkrecht; einzig bei Daten aus allgemein zugänglichen Quellen, die zu Dokumentations-

[15] Vor Inkrafttreten der Justizreform 2007 war die eidgenössische Datenschutzkommission (EDSK/EDÖK) zuständig.

zwecken gespeichert sind, muss auf Verlangen des Betroffenen dessen Gegendarstellung beigefügt werden. Ohne diese dürfen die Daten nicht übermittelt werden. Im allen anderen Fällen gilt: Lässt sich bei Daten weder die Unrichtigkeit noch die Richtigkeit feststellen, so sind die Daten zu sperren (SIR 2010: 61). Dies bedeutet eine Verstärkung des Rechtsschutzes des Betroffenen gegenüber dem Vermerk.

Die Mitteilung und Veröffentlichung einer Sperrung, Berichtigung, Vernichtung oder eines Vermerks ist mit Ausnahme von Österreich und Grossbritannien vorgesehen, wobei in Deutschland nur diejenigen Stellen benachrichtigt werden müssen, an die die Daten weitergegeben wurden. Allerdings muss der Aufwand dafür verhältnismässig sein, und es dürfen keine schutzwürdigen Interessen der betroffenen Person entgegenstehen.

Deutschland kennt ein Widerspruchsrecht: Der Betroffene kann einer Verwendung widersprechen und damit die Bearbeitung verhindern, wenn seine persönlichen Interessen aufgrund seiner besonderen Situation diejenigen der Bearbeitung überwiegen und der Bearbeiter nicht aufgrund einer Rechtsvorschrift verpflichtet ist. Auch Österreich kennt ein Widerspruchsrecht.

Tabelle 7-1: Durchsetzungsrechte der Betroffenen Ländervergleich

	Auskunft	*Sperrung*	*Berichtigung*	*Vernichtung*	*Vermerkung*	*Mitteilung Veröffentlichung*
DE	P,S	P,S	P,S	P,S	P,-	P,S
F	P,S	P,S	P,S	P,S	-,-	P,S
GB	P,S	P,S	P,S	P,S	P,S	-,-
NL	P,S	P,S	P,S	P,S	-,-	P,S
IT	P,S	P,S	P,S	P,S	-,-	P,S
CND	P,S	P,S	P,S	-,-	P,S	P,S
ÖS	P,S	P,S	P,S	P,S	-,-	-,-
SL	P,S	P,S	P,S	P,S	P,S	P,S
ES	P,S	P,S	P,S	P,S	-,-	P,S
CH	*P,S*	*P,S*	*P,S*	*P,S*	*P,S*	*P,S*

P: Durchsetzungsrecht gegenüber privatem Bearbeiter; S: Durchsetzungsrecht gegenüber Staatsorgan. Angaben (ausser CH) basierend auf SIR 2010.

Gegenüber staatlichen Bearbeitern besteht in den meisten Ländern die Möglichkeit, die Unterlassung, die Beseitigung oder die Feststellung der Widerrechtlichkeit zu verlangen. Das gleiche gilt für die Vernichtung, die Sperrung und die Berichtigung der Bearbeitung. Auch die Mitteilung und Veröffentlichungspflicht bei fehlbarer Bearbeitung ist in den meisten Rechtsordnungen verankert.

Ferner besteht in Deutschland sowohl gegenüber Privaten als auch staatlichen Bearbeitern ein Ersatzanspruch, wenn einer betroffenen Person durch eine widerrechtliche Datenbearbeitung Schaden entstanden ist. In Österreich kann der Betroffene auch Schadenersatz für immaterielle Schäden einfordern.

Für die Durchsetzung der Rechte sehen die Länder unterschiedliche Wege vor (Tabelle 7-2). In Deutschland und Slowenien sind wie in der Schweiz sowohl für Bearbeitungen von privaten wie von öffentlichen Bearbeitern ausschliesslich Gerichte anzurufen, in Spanien nur für öffentliche Bearbeiter. In Frankreich und in Spanien ist bei Bearbeitungen von Privaten die Datenschutzbehörde zuständig.

In Grossbritannien, Kanada, Italien, den Niederlanden und Österreich sind sowohl die Datenschutzbehörde als auch Gerichte involviert. In den Niederlanden kann die Datenschutzbehörde zur Mediation oder Meinungsäusserung beigezogen werden. In Italien existieren neben der Beschwerde weitere Formen, mit denen die Datenschutzbehörde angerufen werden kann. In Österreich kommt die Datenschutzbehörde teilweise subsidiär zum Zug, wenn die Voraussetzungen für die Anrufung eines Zivilgerichts nicht erfüllt sind. Bei Verdacht auf eine schwerwiegende Verletzung ist die Kommission zu einer Feststellungsklage verpflichtet. In Grossbritannien kann die betroffene Person sich an die Datenschutzbehörde oder an ein Gericht wenden. In Kanada ist die Datenschutzbehörde die Anlaufstelle, wobei die Weiterbehandlung des Falls auch vor die Gerichte führen kann.

Die zuständigen Instanzen können in mehreren Ländern wie in der Schweiz vorläufige Massnahmen anordnen. In Deutschland sind Vereine bei Datenbearbeitungen von Privaten klageberechtigt. Die Sammelklage ist zwar nicht überall ausgeschlossen, aber nirgends explizit im Datenschutzgesetz vorgesehen.

Tabelle 7-2: Zuständige Instanzen der Rechtsdurchsetzung, Ländervergleich

	Private Bearbeiter	*Öffentliche Bearbeiter*	*Vorsorgliche Massnahme*	*Vereine klageberechtigt oder Sammelklage*
DE	Zivilgericht, Arbeitsgericht, Verwaltungsgericht[a]	Verwaltungsgericht, Sozialgericht, Finanzgericht	P, S	Vereine im Privatbereich klageberechtigt
F	Datenschutzbehörde		keine Angabe	nein
GB	Gericht, Datenschutzbehörde		keine Angabe	nicht ausdrücklich vorgesehen
NL	Zivilgericht Datenschutzbehörde[b]	Verwaltungsgerichtsbarkeit Datenschutzbehörde	keine Angabe	nicht vorgesehen
IT	Gericht, Datenschutzbehörde		ja	nein
CND	Gericht, Datenschutzbehörde		keine Angabe	nicht ausdrücklich vorgesehen
ÖS	Zivilgericht; Datenschutzkommission (tw. von Amtes wegen)		P, S	Sammelklage nicht explizit im DSG geregelt, grundsätzlich nicht unmöglich
SL	Gericht		P,S	nicht vorgesehen
ES	Datenschutzbehörde	Verwaltungsgericht	keine Angabe	nicht ausdrücklich vorgesehen
CH	*Zivilgericht*	*Verwaltungsgericht*	*P, S*	*nein*

P: Gilt gegenüber Bearbeitungen von Privaten, S: Gilt gegenüber Bearbeitungen staatlicher Organe. Angaben (ausser CH) basierend auf SIR (2010).

[a]: Streitigkeiten bezüglich der Überwachung durch Aufsichtsbehörden

[b]: Anfrage zu Mediation oder Meinungsäusserung während einer Auseinandersetzung zwischen Betroffenem und Bearbeiter.

Die Betroffenen von Datenbearbeitungen in der Schweiz sind somit bezüglich ihrer Durchsetzungsrechte ähnlich gut und teilweise sogar besser ausgestattet als die Betroffenen der im Rechtsvergleich untersuchten Staaten. Die deutlichsten Unterschiede bestehen hinsichtlich des Vermerkrechts, das nur in einem Teil der berücksichtigten Länder vorgesehen ist. Eine Verstärkung dieses Rechts zugunsten des Betroffenen kennt Deutschland: Kann die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden, so werden die Daten gesperrt. Damit liegt die Beweislast beim Bearbeiter.

Einzelne Länder kennen im Unterschied zur Schweiz die Möglichkeit der Schadenersatzforderung. Hinsichtlich des Verfahrens gibt es mehrere Länder, die die Rechtsdurchsetzung wie die Schweiz den Gerichten überlassen. In einigen Ländern können Betroffene aber auch die Datenschutzbehörde anrufen oder ergänzend beiziehen.

8 Kenntnis und Durchsetzung der Rechte durch die Betroffenen

Um die Durchsetzungsrechte, die das DSG den Betroffenen in die Hand gibt, auch tatsächlich nutzen zu können, muss – neben den bereits im vorangegangenen Teil vorgestellten Ergebnissen zu Einstellungsfragen – auch das Wissen um die entsprechenden Rechte vorhanden sein. Dieses Kapitel beschäftigt sich deshalb zunächst mit der Frage, ob die Betroffenen das DSG und dessen Inhalt kennen. Dabei stützen wir uns hauptsächlich auf die Ergebnisse aus der Bevölkerungsbefragung, ziehen darüber hinaus aber auch Einschätzungen der Interviewpartner (Experten, EDÖB) zur besseren Einordnung der Befunde bei. In einem zweiten Schritt geht es darum, das Verhalten der Bevölkerung beim (vermuteten) Vorliegen eines Missbrauchsfalles genauer zu beleuchten; daraus lassen sich zumindest partiell Hinweise ableiten, inwiefern die Bevölkerung tatsächlich gewillt und in der Lage ist, ihre Rechte im Falle einer mutmasslichen Verletzung ihrer Persönlichkeitsrechte auf dem Gerichtsweg durchzusetzen. Drittens werden Befunde aus der Analyse der Rechtsprechung vorgestellt, die Aussagen über die quantitative Inanspruchnahme der Durchsetzungsrechte durch die Betroffenen umfassen.

8.1 Kenntnis des Datenschutzgesetzes

Nachfolgend werden zunächst die Resultate aus der Bevölkerungsumfrage zur Bekanntheit des Gesetzes beschrieben. Sie werden zuerst mit Ergebnissen ausländischer Umfrage verglichen, danach werden verschiedene soziodemographische Gruppen verglichen.

8.1.1 Kenntnis des DSG

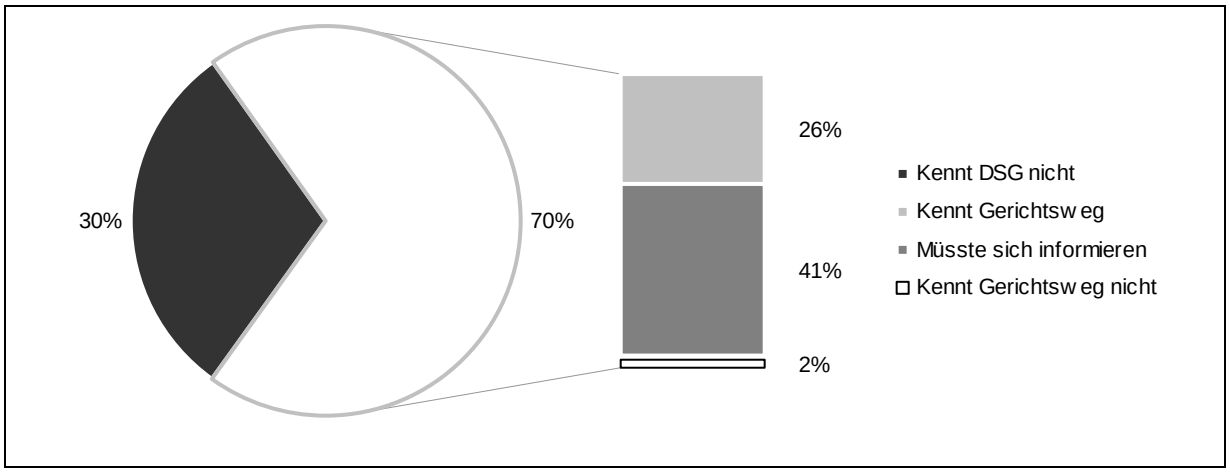
Im Rahmen der Umfrage (vgl. auch Kapitel 5) wurden die Befragten danach gefragt, ob sie vom DSG schon gehört hätten. 70% antworteten mit Ja, 30% gaben an, bisher noch nicht von diesem Gesetz gehört zu haben (Abbildung 8-1). Diejenigen, die angaben, vom Gesetz schon gehört zu haben, wurden danach gefragt, ob sie in Falle eines Missbrauchs ihr Recht vor Gericht durchsetzen könnten. 26% aller Befragten gaben die korrekte Antwort, dass dies zutreffe. 41% aller Befragten zeigten sich unsicher und gaben an, sie müssten sich darüber informieren. 2% verneinten die Möglichkeit, wegen des Missbrauchs das Gericht anzurufen.

Auch die Interviewpartner äussern sich dahingehend, dass in der Bevölkerung bezüglich der Kenntnisse des DSG und insbesondere der Durchsetzungsrechte Lücken bestehen. Beide Rechtsexperten vermuten, dass die überwiegende Mehrheit der Betroffenen die Möglichkeiten zur Durchsetzung ihrer Rechte im Falle einer Datenschutzverletzung nicht kennen oder mit der Anwendung im konkreten Einzelfall überfordert sind. Die Einschätzung der Interessenvertreter fällt ähnlich aus.

Im Rahmen der Eurobarometer-Umfrage (Eurobarometer 2008) wurde die EU-Bevölkerung noch differenzierter zu ihren datenschutzbezogenen Rechten im jeweiligen Land befragt. Auch dort zeigten sich teilweise Lücken in den Kenntnissen des Gesetzes. Insofern fällt die schweizerische Bevölkerung diesbezüglich nicht aus dem Rahmen. 27% der Befragten kannten gemäss die-

ser Umfrage sämtliche Rechte, die ihnen zur Verfügung stehen.[16] Im Gegensatz zu den Aussagen der Rechtsexperten wird dabei jedoch die Dimension nicht erfasst, dass es nicht nur darauf ankommt, die zur Verfügung stehenden Rechte zu kennen, sondern auch, wie man im Einzelfall konkret vorzugehen hat. Dies erfordere einiges an juristischem Verständnis, das bei der Bevölkerung in der Regel fehlen dürfte. Mitunter könnte auch ein gewisser Respekt vor dem Rechtsweg vorhanden sein.

Abbildung 8-1: Kenntnis des DSG und der Durchsetzungsrechte



N = 1014. Lesehilfe: 70% der Befragten (weisse Fläche) haben vom DSG schon gehört. In dieser Gruppe bejahten 26% die Zusatzfrage, ob man gegen einen Verstoss gegen das DSG vor Gericht gehen kann. 41% gaben bei der Zusatzfrage an, sie müssten sich zuerst informieren, 1% verneinten die Möglichkeit des Gerichtswegs (keine Antwort/weiss nicht: 1%). Genaue Fragestellung vgl. Anhang 2.

8.1.2 Bekanntheit des DSG nach sozialen Gruppen

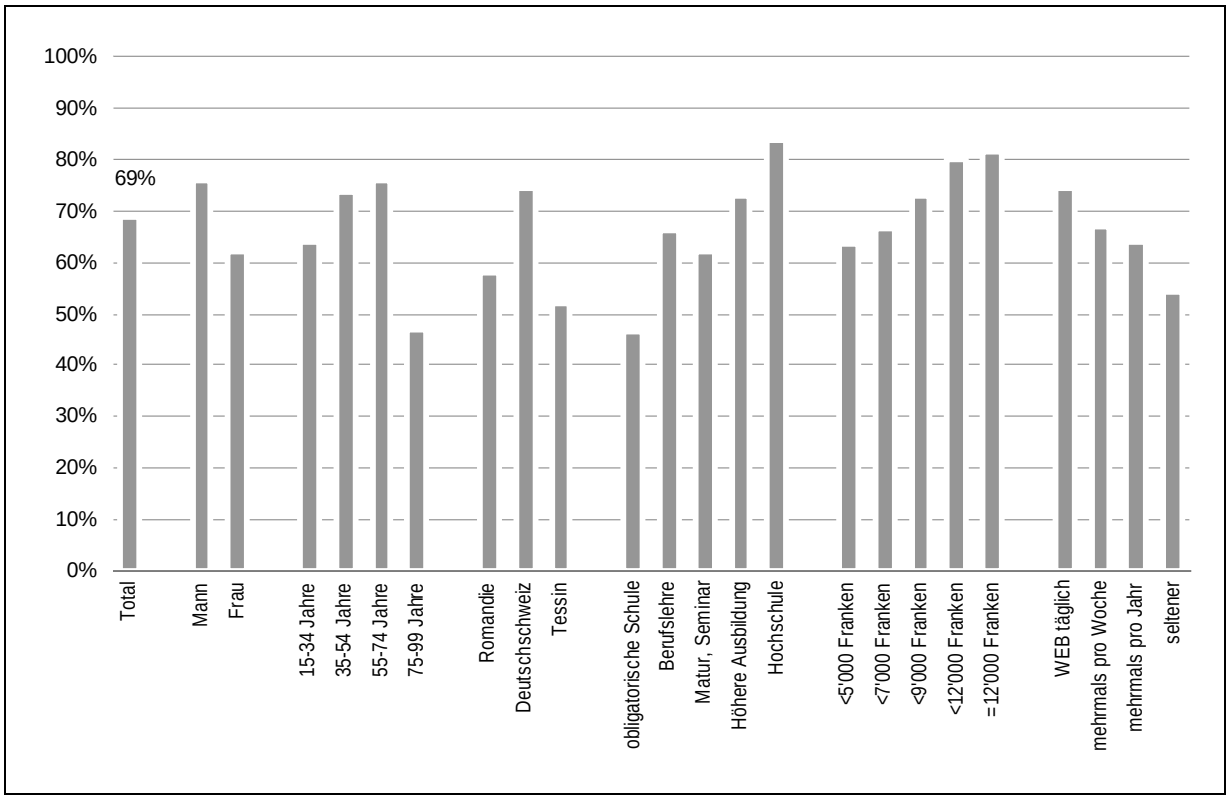
Hinsichtlich der Bekanntheit des DSG bestehen deutliche Unterschiede zwischen den verschiedenen soziodemographischen Gruppen. Abbildung 8-2 lässt klare Tendenzen erkennen. Männer haben vom DSG häufiger gehört als Frauen, Personen mit hohem Bildungsniveau und Einkommen häufiger als Personen mit niedrigem Bildungsniveau und Einkommen. Auch regelmässigen Nutzern des Internet ist das DSG häufiger bekannt als Personen, die sich selten im Netz bewegen. Sprachregional gesehen ist die Bekanntheit des Gesetzes im Tessin und in der Romandie tiefer als in der Deutschschweiz.

Hinsichtlich des Alters lässt sich mit steigendem Alter eine zunehmende Bekanntheit des DSG bei den verschiedenen Altersgruppen feststellen. Eine Ausnahme bildet die Gruppe der 75-99jährigen: nicht einmal jeder zweite kennt das Gesetz. Eine mögliche Erklärung für diesen Befund könnte die Tatsache liefern, dass das DSG erst im Jahr 1993 eingeführt worden ist. Alle

[16] In der Eurobarometer-Umfrage wurden die interviewten Personen zu den Rechten, die ihnen aufgrund der Datenschutzgesetzgebung zustehen, befragt. Konkret handelt es sich dabei um das Recht, einer Datenbearbeitung zu widersprechen (88% gaben an, dass sie dieses Recht zur Verfügung haben), die Notwendigkeit einer Einwilligung für gewisse Datenbearbeitungen (81%), das Berichtigungs- und Löschrecht bei falschen Daten (78%), der Zugang

beschriebenen Gruppenunterschiede sind statistisch signifikant mit einer Irrtumswahrscheinlichkeit von maximal 5%.

Abbildung 8-2: Bekanntheit des DSG, nach sozialen Gruppen



N = 1014. Genaue Fragestellung vgl. Anhang 2.

8.2 Verhalten im Missbrauchsfall

Wurde mit der oben erläuterten Frage die *passive* Kenntnis des Gesetzes („Haben sie vom DSG schon gehört?“) erfragt, steht hier das Verhalten der Betroffenen in einem erlebten oder hypothetischen Missbrauchsfall im Vordergrund. Es interessiert, inwieweit die Betroffenen die Möglichkeiten, die ihnen das Datenschutzgesetz bieten, *aktiv* kennen und auch anwenden. Zuvor ist kurz auf die von den Befragten berichteten Missbrauchserlebnisse einzugehen. Sie geben einerseits gewisse Aufschlüsse über die quantitative Bedeutung verschiedener Missbrauchsformen, andererseits auch Hinweise darüber, was die Teilnehmerinnen und Teilnehmer der Umfrage unter dem Begriff des Missbrauchs verstehen.

8.2.1 Als Missbrauch erlebte Datenbearbeitungen

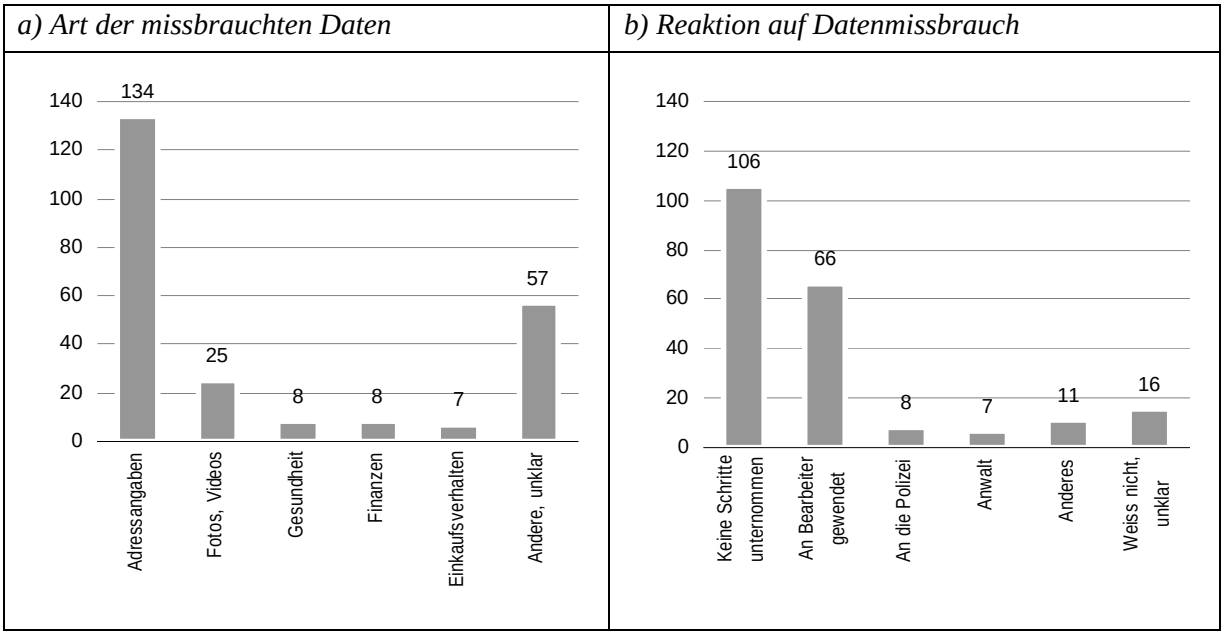
In der Umfrage von Privatim (2009) gaben 15% der Personen an, sie seien schon einmal von einem Missbrauch ihrer Daten betroffen gewesen. Die hier durchgeführte Umfrage kommt dies-

zur Rechtspflege im Falle einer Datenschutzverletzung (71%), das Recht auf Kompensation im Falle einer Datenschutzverletzung (61%) und das Auskunftsrecht (59%). Insgesamt kennen 27% alle Rechte.

bezüglich zu einem ähnlichen Resultat. Auf die Frage: „Ist es schon vorgekommen, dass jemand persönliche Angaben von Ihnen gesammelt oder auf eine Art und Weise verwendet hat, wo Sie das Gefühl hatten, das geht nun wirklich nicht, das ist nicht zulässig?“ antworteten 21% der Befragten mit Ja. Die Nachfrage nach der Art der Daten, die missbraucht worden sind, zeigt, dass die Befragten in mehr als der Hälfte der Fälle den Umgang mit ihren Adressdaten als missbräuchlich empfunden haben. Diese Form von Datenbearbeitung ist zwar hinsichtlich ihrer Folgen meist vergleichsweise harmlos. Sie stellt aber in den Augen der Betroffenen offensichtlich weitaus die häufigste Grenzüberschreitung dar, während andere Missbräuche seltener erlebt werden. Ebenfalls relativ häufig wird der Missbrauch von Fotos oder Videodaten genannt.

Petersen (2010) kommt für Deutschland zum Schluss, dass die Bevölkerung Datenmissbrauch weit definiert und teils auch legale Praktiken darunter subsumiert. Dies kann angesichts der hier vorgefundenen Resultate und Angaben über die missbrauchten Daten für die Schweiz ebenfalls angenommen werden. Gleichzeitig können die Befragten nur von Missbräuchen berichten, die sie bemerkt haben. Insofern spiegelt der hier angegebene Wert von 21% die Empfindung der Bevölkerung und nicht das tatsächliche Missbrauchsniveau, das kaum beziffert werden kann.

Abbildung 8-3: Datenmissbrauch: Art und Reaktion



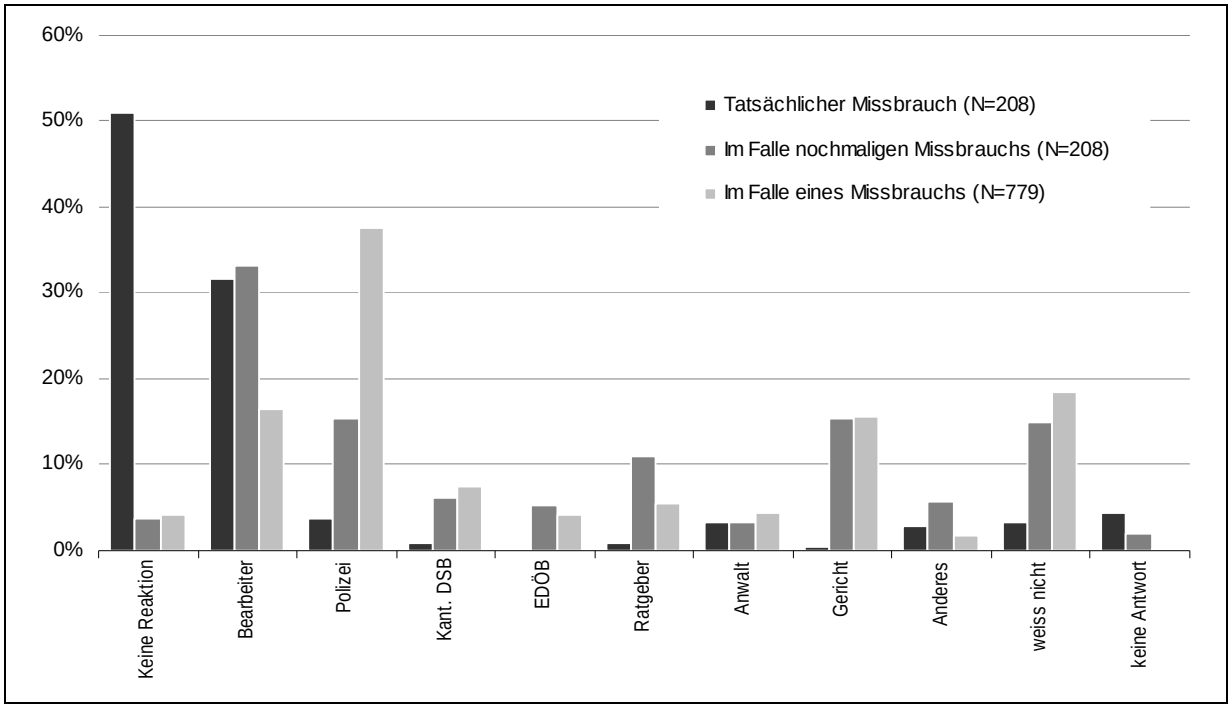
a) N = 208 von 1014 befragten Personen und 239 genannte Arten von Daten. b) N = 208 von 1014 befragten Personen und 214 genannte Reaktionen auf einen Missbrauch. Genaue Fragestellung vgl. Anhang 2.

Inwiefern sich die genannten missbräuchlichen Datenbearbeitungen auf neue, unübersichtliche und intransparente Konstellationen beziehen, lässt sich nicht mit Sicherheit sagen. Es ist jedoch zu vermuten, dass es sich bei den von den Befragten genannten Missbrauchsfällen nicht zuletzt aufgrund der grossen Bedeutung von Adressangaben eher um klassische Situationen handelt.

8.2.2 Reaktion auf erlebten und hypothetischen Missbrauch

Die vom Missbrauch betroffenen Personen wurden auch nach ihrer Reaktion auf einen Datenmissbrauch gefragt. Ihren Aussagen zufolge haben sie in gut der Hälfte der Fälle keine konkreten Schritte unternommen, um den Missbrauch zu unterbinden. Von den übrigen hat sich der überwiegende Teil direkt an den Bearbeiter gewendet, seltener auch an die Polizei oder einen Anwalt. Zwei Personen gaben an, sie hätten sich an den kantonalen Datenschutzbeauftragten gewendet, eine gab an, sie sei vor Gericht gegangen. Der EDÖB wurde nicht erwähnt.

Abbildung 8-4: Reaktion auf tatsächlichen und allfälligen Datenmissbrauch



N= 1014 Befragte (208 Personen mit einem berichteten Missbrauchserlebnis und 779 Personen, welche über kein Missbrauchserlebnis berichteten. 27 Personen antworteten auf die Frage nach einem Missbrauchserlebnis mit „weiss nicht“). Genaue Fragestellung vgl. Anhang 2.

Das passive Verhalten im konkreten Missbrauchsfall eines bedeutenden Teils der Befragten mag bis zu einem gewissen Grad durch die Tatsache erklärbar sein, dass es häufig um Adressdaten und somit einen vergleichsweise harmlosen Sachverhalt ging. Gleichwohl erstaunt, wie stark dieses tatsächliche Verhalten mit dem deklarierten Verhalten in einem hypothetischen Fall kontrastiert. So wurden die von einem Missbrauch bereits betroffenen Personen gefragt, wie sie sich verhalten würden, wenn sie neuerlich einen Missbrauch erleben würden. Sie zeigten sich im Vergleich zu ihrem tatsächlichen Verhalten im Falle einer erneuten Missbrauchserfahrung deutlich entschlossener: Statt rund 50% gaben weniger als 5% gab an, nicht auf den Missbrauch reagieren zu wollen, wobei gleichzeitig rund 15% einräumten, nicht zu wissen, wie sie reagieren würden. Rund ein Drittel gab an, sich direkt an den Bearbeiter zu wenden, zwischen 10 und 20% gaben an, sich an die Polizei, an ein Gericht oder an einen Ratgeber (z.B. eine Konsumentenschutzor-

ganisation) wenden zu wollen. Selten werden die Datenschutzbeauftragten von Kanton und Bund oder ein persönlicher Anwalt genannt.

Noch kämpferischer zeigten sich in der Umfrage diejenigen Personen, die über bisher keine Missbrauchserfahrung berichteten. Sie wurden ebenfalls nach ihrer Reaktion gefragt, „wenn Sie einmal in eine solche Situation geraten, dass persönliche Daten von Ihnen missbraucht werden". Mehr als ein Drittel dieser Personen erklärten, sie würden sich an die Polizei wenden. Zwischen 10 und 20% dieser Gruppe würde sich direkt an den Datenbearbeiter oder an ein Gericht wenden. Auch in dieser Gruppe sind Anwälte und Datenschutzbeauftragte (wie auch andere Ratgeber) nur für eine kleine Minderheit eine wichtige Anlaufstelle. 18% gaben an, sie wüssten nicht, wie sie sich verhalten würden. Zu beachten gilt es, dass der Vergleich zwischen dem realen und dem hypothetischen Verhalten in einem Missbrauchsfall mit einer gewissen Vorsicht zu ziehen ist: Der Effekt der sozialen Erwünschtheit beim Antwortverhalten dürfte bezüglich der hypothetischen Reaktion stärker zum Ausdruck kommen. Die Unterschiede bleiben jedoch auch unter Berücksichtigung dieses Effekts beträchtlich.

Diese Antwortmuster stützen die Experten, welche in den Interviews die Betroffenen bei der Ausübung ihrer Durchsetzungsrechte teilweise als überfordert bezeichneten. Diese Sichtweise spiegelt sich einem hohen Anteil an Personen, die trotz der subjektiv empfundenen Verletzung ihrer Persönlichkeitsrechte keine aktiven Schritte gegen den erlebten Missbrauch unternehmen. Im hypothetischen Missbrauchsfall dagegen zeigt sich eine sehr viel stärkere Bereitschaft, gegen den Missbrauch vorzugehen und allenfalls sogar vor Gericht zu gehen. Diese Befunde deuten darauf hin, dass die Bevölkerung durchaus am Schutz ihrer persönlichen Daten interessiert ist und deren Missbrauch als stossend empfindet (vgl. Kapitel 5).

Das hier vorgefundene Antwortmuster deckt sich teilweise, aber nicht vollständig mit jenem der Umfrage von Privatim (2009). In dieser Befragung gaben 40% der Befragten an, sie würden sich an die Polizei wenden und 35%, sie würden sich an den Bearbeiter wenden. Deutlich häufiger als in der hier durchgeführten Umfrage werden Datenschutzbeauftragte (26%) und Konsumentenschutzorganisationen (21%) als Anlaufstelle genannt. Dies dürfte daran liegen, dass dort die Antwortkategorien vorgelesen wurden, in der hier vorgelegten Umfrage hingegen Spontannennungen entgegengenommen wurden.

Das Antwortverhalten in der vorliegenden Umfrage verdeutlicht somit stärker als die Privatim-Studie, dass die vorgesehenen Rechtswege, die staatlichen Datenschutzbeauftragten und andere Unterstützungsmöglichkeiten im Bewusstsein der Bevölkerung nicht sonderlich stark verankert sind, und dass die Polizei als erste Anlaufstelle für alle Belange der persönlichen Sicherheit und somit auch des Datenschutzes wahrgenommen wird.

Dass Personen ohne Missbrauchserlebnis sich vergleichsweise entschlossen zu einer Reaktion zeigen, kann daran liegen, dass sie sich die Reaktion auf einen Missbrauch einfacher vorstellen, als jene Personen, die mit der Situation bereits konfrontiert wurden. Es könnte aber auch daran liegen, dass sich diese Personen sich unter einem Missbrauch ein gravierenderes Vergehen vorgestellt haben als jene Missbrauchsfälle, um die es sich für viele der 208 Personen mit Missbrauchserfahrung gehandelt hat.

8.3 Inanspruchnahme der Durchsetzungsrechte: Quantitative Analyse der Rechtsprechung

Ziel dieses Abschnitts ist es, einen Überblick zu geben, wie oft und mit welcher Erfolgsquote die Betroffenen die Einsichts- bzw. Auskunftsrechte (Art. 8 ff. DSG) und die Durchsetzungsrechte (Art. 15, Art. 25 DSG) anrufen. Bereits an dieser Stelle ist vorwegzunehmen, dass die Durchsetzungsrechte im Sinne von Art. 15 und Art. 25 DSG vor dem Bundesverwaltungsgericht (seit 2007), vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission (bis 2006), vor den kantonalen Behörden und auch vor dem Bundesgericht im Vergleich etwa zu Auskunftsbegehren nach Art. 8 Abs. 1 DSG (bzw. den entsprechenden Artikeln der kantonalen Datenschutz- oder Spezialgesetze; vgl. Ziffer 9.1.2) sehr selten geltend gemacht werden. Von den vergleichsweise wenigen Fällen, die sich auf die Durchsetzungsrechte stützten, betrafen die meisten Ansprüche Art. 25 DSG und insbesondere Berichtigungsgesuche, so dass der Analyse der Rechtsprechung zu Art. 25 DSG ein etwas stärkeres Gewicht zukommen soll.

Für die quantitative Analyse wurden 269 Fälle herangezogen, die vor die kantonalen und eidgenössischen Gerichte gebracht wurden (vgl. Ziffer 8.3.1 ff.). Die kantonalen Behörden beurteilen die vorgebrachten Fälle zum Datenschutzrecht nach den kantonalen Datenschutzgesetzen oder weiteren einschlägigen kantonalen Bestimmungen, d.h. nicht nach dem DSG. Die kantonalen Gerichte nahmen jedoch immer wieder auf das Datenschutzgesetz des Bundes Bezug, um (unklare) kantonale Bestimmungen zum Datenschutz auszulegen.

Mittels der Suchfunktion auf der jeweiligen offiziellen Entscheiddatenbank wurden die Urteile vor Bundes-[17] bzw. Bundesverwaltungsgericht[18] zu Art. 8, 15 und 25 DSG ermittelt. Die Entscheide der Eidgenössischen Datenschutz- und Öffentlichkeitskommission sind vollständig im Internet einsehbar[19]. Hinsichtlich der kantonalen Urteile wurden die zuständigen kantonalen Behörden angefragt, sämtliche nicht im Internet verfügbaren Urteile zur Verfügung zu stellen, die datenschutzrechtliche Erwägungen beinhalteten. Diese sind zusammen mit den im Internet abrufbaren kantonalen datenschutzrechtlichen Urteilen zu einer Datenbank zusammengefügt worden und können auf der Homepage des Instituts für Europarecht der Universität Freiburg eingesehen werden[20]. Aufgrund der Vorgehensweise kann davon ausgegangen werden, dass damit ein repräsentativer Teil der durch die schweizerischen Gerichte zu den erwähnten Artikeln ergangenen Urteile berücksichtigt werden konnte[21].

[17] http://www.bger.ch.
[18] http://www.bvger.ch/publiws/?lang=de.
[19] http://www.fir.unisg.ch/Datenschutz/index.html.
[20] http://www.unifr.ch/euroinstitut/de/aktivitaeten/datenbank.
[21] Für das Bundesgericht wurden Urteile zwischen 1993 und 2010 berücksichtigt, für die Eidgenössische Datenschutz- und Öffentlichkeitskommission von 1993-2006 und für das Bundesverwaltungsgericht von 2007-2010. Die betrachteten kantonalen Fälle reichen bis Anfang der 80er Jahre zurück.

8.3.1 Inanspruchnahme des Auskunftsrechts (Art. 8 DSG)

Im Rahmen der hier analysierten Rechtsprechung entfiel eine grosse Anzahl geltend gemachter Rechtsansprüche auf das Auskunftsrecht im Sinne von Art. 8 DSG (bzw. auf kantonalen Bestimmungen zum Auskunftsrecht).

In 28 Fällen vor dem Bundes- bzw. Bundesverwaltungsgericht verlangten Betroffene Auskunft über bzw. Einsicht in die über sie bearbeiteten Daten gemäss Art. 8 DSG[22]; dazu eine Vergleichszahl: Zum Stichwort DSG ergingen vor dem Bundes- bzw. dem Bundesverwaltungsgericht insgesamt 72 Urteile. Besonders häufig waren Einsichtsgesuche vor den höchsten Gerichten im Asylbereich (13 Fälle; insbesondere nach abgeschlossenem Asylverfahren). Weitere Fallgruppen ergaben sich für den Bereich Hochschulen und Kranken- bzw. Unfallversicherungen.

Auch die Rechtsprechung der Eidgenössischen Datenschutz- und Rekurskommission (1993-2006) behandelte in einem grossen Teil der Fälle (zwanzig Fälle von insgesamt 85 Urteilen) Fragen zum Einsichtsrecht nach Art. 8 DSG. Thematisch betrafen die Fälle den Asylbereich, die Rechts- und Amtshilfe, die Einsicht in medizinische Dossiers und das Bundespersonalrecht.

In rund der Hälfte der Fälle wurde die Auskunft durch das Bundes- bzw. Bundesverwaltungsgericht gewährt; vor der Rekurskommission wurde den Auskunftsbegehren sogar in der Mehrzahl der Fälle stattgegeben. Die Erfolgsquote (d.h. erfolgreich geltend gemachte Beschwerden) im Bereich der Einsichtsrechte nach Art. 8 DSG liegt damit viel höher als bei der Geltendmachung der Durchsetzungsrechte nach Art. 15 und 25 DSG[23].

In den Fällen, in denen die Auskunft abgelehnt oder eingeschränkt wurde, geschah dies bei den Urteilen vor höheren Gerichten zum grössten Teil auf der Grundlage einer Interessenabwägung gemäss Art. 9 DSG. Einigen Einsichtsgesuchen konnte nicht stattgegeben werden, weil das Gesuch – auch nach der mehrmaligen Aufforderung, es zu substantiieren – ungenügend begründet war. Dies betraf Fälle, bei denen der Beschwerdeführer eine Bearbeitung seiner Personendaten zwar behauptete, aber nicht begründen oder spezifizieren konnte, worauf er den Verdacht einer Bearbeitung seiner Daten stützte. Die Gerichte verlangten in diesem Fall zumindest eine Angabe, welche Behörde die Daten angeblich bearbeitet hatte, um dort Abklärungen treffen zu können. Wenn auch die Angaben zu der vermutungsweise bearbeitenden Behörde ausblieben, konnten die Gerichte nicht eintreten[24].

Auch bei den kantonalen Entscheiden im Bereich des Datenschutzes (insgesamt 112 Entscheide) betraf – ebenso wie auf Bundesebene – ein Grossteil der Urteile (35 Fälle) Streitpunkte zu den Auskunfts- bzw. Einsichtsrechten. Ungefähr in zwei Dritteln der Urteile wurden die Beschwerden abgewiesen.

Zu beachten ist bei den kantonalen Entscheiden zum datenschutzrechtlichen Auskunftsrecht die thematische Vielfalt der Fälle, die sich erst vor höheren Instanzen auf typische Fallgruppen reduziert. Die kantonalen Einsichtsrechtsfälle betrafen unter anderem die Akteneinsicht bei Patien-

---

22 In einigen Fällen stützten sie sich für die Geltendmachung der Einsicht auch direkt auf die BV bzw. auf das VwVG. Ähnlich viele Fälle ergingen nur zum Berichtigungsanspruch nach Art. 25 DSG, dazu unten.

23 Vgl. Ziffer 8.3.2 f..

24 VPB 67.70.

tendossiers, die Einsichtnahme in Schülerakten einer Volksschule, die Einsichtnahme ins Zivilstandsregister zwecks Ahnenforschung[25], die Herausgabe von Adressen aus dem Stimmregister zwecks Gründung eines Ortsvereins und viele mehr.

Vor kantonalen Instanzen wurde – anders als auf Bundesebene – die Mehrzahl der Einsichtsgesuche abgewiesen.

8.3.2 Durchsetzungsrechte gegenüber Privaten (Art. 15 DSG)

Vor dem Bundes- und Bundesverwaltungsgericht wurde nur ein Fall gefunden, im dem der Kläger (erfolglos) die Widerrechtlichkeit der Veröffentlichung eines Artikels über ihn und die Verwendung eines Bildes von ihm in einer Wochenzeitschrift gemäss Art. 28 ff. ZGB feststellen lassen wollte. Art. 15 DSG wurde dabei zumindest vor dem Bundesgericht nicht explizit erwähnt[26]. Gestützt auf Art. 15 DSG im Sinne eines Durchsetzungsrechts konnte demnach vor dem Bundes- bzw. Bundesverwaltungsgericht keiner der Beschwerdeführer erfolgreich gegen die Datenbearbeitung durch einen Privaten vorgehen.

Vor der Eidgenössischen Datenschutz- und Rekurskommission wurde in einigen Urteilen auf Art. 15 DSG Bezug genommen, jedoch nicht im Sinne eines Durchsetzungsrechts:

- Unter Bezugnahme auf Art. 15 Abs. 2 DSG erging vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission das Urteil Nr. 18/05 vom 28. Dezember 2006; dabei ging es insbesondere um die Handhabung des Anbringens eines Bestreitungsvermerks bzw. um Fragen der Beweislast. Art. 15 DSG wurde jedoch nicht als Durchsetzungsrecht angerufen.
- Im Entscheid Nr. 4/01 der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 22. Mai 2003/15. März 2004 zum Verfahren betreffend die Auskunft gemäss BWIS/ZentG erfolgte nur eine vergleichende Bezugnahme auf Art. 15 DSG durch das Gericht. Art. 15 DSG wurde nicht im Sinne des Durchsetzungsrechts geltend gemacht.
- Im Urteil Nr. 05/03 der Eidgenössischen Datenschutzkommission vom 15. April 2005 (= VPB 69.106) wurde die unerbetene Zusendung von Werbung mittels E-Mail (so genannte „Spam-Mails“) datenschutzrechtlich beurteilt; es erfolgte ebenfalls nur ein Verweis auf den Art. 15 DSG.

Vor den kantonalen Gerichten ergaben sich sechs Urteile mit Bezug auf die Datenbearbeitung durch Private; drei der vorgebrachten Beschwerden wurde gutgeheissen.

Insgesamt konnten auch nur sehr wenige, und vor dem Bundesgericht nur ein einziges Urteil gefunden werden, in welchem gestützt auf Art. 15 DSG i.V.m. Art. 28c ZGB vorsorgliche Massnahmen beantragt wurden[27]. Auch hierbei kam Art. 15 DSG als Anspruchsgrundlage keine Bedeutung zu.

---

[25] Unter einschränkenden Bedingungen wurde einem Gesuchsteller die Einsicht in ein Zivilstandsregister für die Ahnenforschung gewährt; seine Beschwerde gegen den vorinstanzlichen Entscheid wurde teilweise gutgeheissen. Entscheid des Baudepartements des Kantons Solothurn vom 2.7.1996.

[26] BGE 127 III 481, dazu unten.

[27] BGr. 4P.293/2006, Urteil vom 9.2.2007; vgl. Ziffer 9.3.1.

Zusammenfassend kann festgehalten werden, dass die Beschwerdeführer bei der Hälfte der kantonalen Urteile und bei der überwiegenden Mehrzahl aller betrachteten Fälle vor den höheren Instanzen bei der Geltendmachung von Verletzung von Persönlichkeitsrechten aufgrund der widerrechtlichen Datenbearbeitung seitens Privater nicht erfolgreich waren.

8.3.3 Durchsetzungsrechte gegenüber Bundesorganen (Art. 25 DSG)

Vergleicht man die Fälle, die gestützt auf die Durchsetzungsrechte von Art. 15 und Art. 25 DSG vor die Gerichte gebracht wurden, so zeigt sich, dass sich diese – obwohl die Durchsetzungsrechte allgemein sehr selten angerufen werden – am häufigsten auf Art. 25 DSG stützen.

Vor dem Bundes- bzw. Bundesverwaltungsgericht wurden in 24 Fällen Ansprüche aus Art. 25 DSG geltend gemacht (als Vergleich die Referenzgrösse: zum Stichwort DSG ergingen insgesamt 72 Urteile vor dem Bundes- und Bundesverwaltungsgericht). Auf den ersten Blick scheint diese Anzahl als relativ gross, jedoch beziehen sich die gestützt auf Art. 25 DSG vorgebrachten Beschwerden auf jeweils ähnliche Sachverhaltskonstellationen, die nachfolgend noch dargestellt werden.

Die gestützt auf Art. 25 DSG ergangenen Beschwerden betrafen in einer deutlichen Mehrzahl (16 Fälle) die Berichtigung im Sinne von Art. 25 Abs. 3 Bst. a DSG[28]. Einer dieser 16 Fälle betraf zusätzlich die Vernichtung und Sperrung im Sinne von Art. 25 Abs. 3 Bst. a DSG (Urteil A-7368/2006 des Bundesverwaltungsgerichts). Die 16 Begehren, welche die Berichtigung im Sinne von Art. 25 Abs. 3 Bst. a DSG zum Gegenstand hatten, waren teilweise erfolgreich und teilweise musste ein Bestreitungsvermerk angebracht werden. 12 von insgesamt 16 Fällen – die überwiegende Mehrzahl der Fälle – betrafen den Asylbereich, und darin sehr ähnliche Sachverhaltskonstellationen[29].

Die übrigen Ansprüche aus Art. 25 DSG (d.h. die Rechtsansprüche ausser Berichtigungen) wurden deutlich seltener geltend gemacht; sie wurden jeweils lediglich in 1-2 Fällen angerufen, die im Überblick kurz angeführt werden sollen:

- 2 Fälle betrafen die Unterlassung im Sinne von Art. 25 Abs. 1 Bst. a DSG. Beide Beschwerden, welche die Unterlassung im Sinne von Art. 25 Abs. 1 Bst. a DSG zum Gegenstand hatten, blieben ohne Erfolg (Urteile A-2482/2007 und A-7372/2006 des Bundesverwaltungsgerichts).
- Ein Fall hatte die Unterlassung, Beseitigung und Feststellung im Sinne von Art. 25 Abs. 1 Bst. a-c DSG zum Gegenstand. Auch diese Beschwerde blieb ohne Erfolg (BGE 122 IV 139).
- Ein Fall betraf die Feststellung der Widerrechtlichkeit einer Bearbeitung im Sinne von Art. 25 Abs. 1 Bst. c DSG. Die Beschwerde war erfolglos (BGE 131 II 413).

[28] Urteile 1A.295/2005, 1A.6/2001, 1C_111/2010 des Bundesgerichts und die Urteile A-4615/2009, A-2168/2009, A-3224/2010, A-6559/2008, A-5737/2007, A-4202/2007, A-7757/2006, A-1507/2009, A-5795/2007, A-1001/2008, A-50/2009, A-3181/2008, A-7368/2006 des Bundesverwaltungsgerichts.

- Zwei Fälle hatten die Vernichtung im Sinne von Art. 25 Abs. 3 Bst. a DSG zum Gegenstand. Dabei war eine der Beschwerden teilweise erfolgreich (Urteile A-6067/2008 und A-3893/2009 des Bundesverwaltungsgerichts).
- Ebenso hatten 2 Fälle die Sperrung im Sinne von Art. 25 Abs. 3 Bst. a DSG zum Inhalt. Beide Beschwerden blieben erfolglos (Urteil 1C 201/2007 des Bundesgerichts und A-4114/2008 des Bundesverwaltungsgerichts).
- In einem Fall schliesslich wurden sämtliche Ansprüche des Art. 25 DSG geltend gemacht. Die Beschwerde blieb ebenfalls ohne Erfolg (Urteil A-4114/2008 des Bundesverwaltungsgerichts)

Hinsichtlich der Erfolgsquote der auf Art. 25 DSG gestützten Fälle lässt sich somit feststellen, dass nur die Geltendmachung der Berichtigungs- und Vernichtungsansprüche zumindest teilweise erfolgreich war[30].

Auch vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission ergab sich bei den Fällen zur Durchsetzung der Rechte nach Art. 25 DSG eine relative Häufung, insbesondere bezüglich Berichtigungsbegehren. Die meisten Berichtigungsbegehren waren erfolgreich; dazu im Überblick die ergangenen Urteile:

- Urteil Nr. 02/99 vom 16. Oktober 2000 (=VPB 66.51) zum schutzwürdigen Interesse im Sinne von Art. 25 Abs. 1 DSG), wonach die Datensammlungen des Bundesamtes für Flüchtlinge für Asylbewerber die Funktion eines „provisorischen" Zivilstandsregisters hätten. Für eine Berichtigung der darin enthaltenen Personendaten genüge ein schutzwürdiges Interesse im Sinne von Art. 25 Abs. 1 DSG; die Beschwerde wurde gutgeheissen.
- Urteil Nr. 01/00 vom 22. Dez. 2000, dieses Verfahren hatte die Berichtigung des (strittigen) Namens eines Asylbewerbers zum Gegenstand und thematisierte ebenfalls Fragen zum schutzwürdigen Interesse; die Beschwerde wurde teilweise gutgeheissen.
- Entscheid 3/02 des Präsidenten der Eidgenössischen Datenschutzkommission vom 14. April 2003 (=VPB 67.74) zur Berichtigung eines Personennamens und zur unentgeltlichen Rechtspflege; diese Beschwerde wurde abgewiesen.
- Urteil Nr. 13/01 vom 4. März 2003 (=VPB 67.72) zur Beweislast nach Art. 25 Abs. 2 DSG; in diesem Urteil wurde festgehalten, dass bei der Anfechtung von bereits registrierten Daten (i.c. im automatisierten Personenregistratursystem AUPER 2) der Beweis der Unrichtigkeit der betroffenen Person obliege und derjenige der Richtigkeit dem Bundesorgan, das Inhaber der Datensammlung sei; die Beschwerde wurde gutgeheissen.
- Urteil Nr. 04/02 vom 16. April 2004 zur Berichtigung von persönlichen Daten mit dem Vermerk, dass deren Richtigkeit bestritten sei; die Beschwerde wurde abgewiesen.

---

[29] Nicht den Asylbereich betrafen die Urteile 1A.295/2005 (ASTRA), 1A.6/2001 (Versicherung), 1C_111/2010 (Strafregister) des Bundesgerichts und A-5795/2007 (Einbürgerung) des Bundesverwaltungsgerichts.

[30] Teilweise erfolgreich bedeutete bei den Berichtigungsansprüchen insbesondere, dass ein Bestreitungsvermerk im Sinne von Art. 25 Abs. 2 DSG angebracht werden musste.

- Urteil Nr. 13/04 vom 12. Dezember 2006 zur Berichtigung von Personendaten im Zentralen Migrationsinformationssystem; diese Beschwerde wurde gutgeheissen.
- Urteil Nr. 16/05 vom 23. August 2006 zur Berichtigung des Geburtsdatums einer Asylbewerberin im automatisierten Personenregistratursystem (AUPER 2); die Beschwerde wurde gutgeheissen.
- Urteil Nr. 4/02 vom 16. April 2004 zur Anbringung eines Bestreitungsvermerks, der auch Dritten mitzuteilen war (Art. 25 Abs. 3 Bst. a DSG); vgl. zum Bestreitungsvermerks nach Art. 25 Abs. 2 DSG auch Urteil Nr. 1/03 zur Berichtigung von Personendaten nach Art. 25 Abs. 2 DSG im automatisierten Personenregistratursystem (AUPER 2); die Beschwerden wurden teilweise gutgeheissen, teils abgewiesen.
- Urteil Nr. 9/03 vom 23. März 2005 zur Berichtigung des Eintrags im automatischen Personenregistratursystem (AUPER 2); in diesem Urteil wurde festgehalten, dass es keines gesonderten Nachweises bedürfe, um sich auf ein schützenswertes Interesse an der Berichtigung der vom BFF (Bundesamt für Flüchtlinge, neu: Bundesamt für Migration, BFM) bearbeiteten Daten zu berufen; die Beschwerde wurde teilweise gutgeheissen.
- Urteil Nr. 06/06 vom 24. August 2006 zur Bestätigung der Praxis, wonach eine Bundesbehörde, welche Personendaten bearbeite, grundsätzlich dafür verantwortlich sei, die Richtigkeit der bearbeiteten Daten zu beweisen, wenn diese bestritten würden. Der betroffenen Person obliege hingegen der Beweis der Unrichtigkeit; dieser Beweis war i.c. nicht erfolgreich, weswegen die Beschwerde abgewiesen wurde.
- Urteil Nr. 02/06 vom 11. Dezember 2006 über die Korrektur des Geburtsdatums im AUPER2 bei Ungewissheit über das wahre Geburtsdatum; die Beschwerde wurde teilweise gutgeheissen.
- Urteil Nr. 18/05 vom 28. Dezember 2006; eine Korrektur von Personendaten könne gemäss Art. 25 DSG nur verlangt werden, wenn die Angaben entweder unrichtig seien oder wenn sie zwar zutreffen würden, die Veröffentlichung dieser aber unverhältnismässig sei; die Beschwerde gegen das Bundesamt für Polizei (BAP; heute fedpol) wurde gutgeheissen.
- Urteil Nr. 6/01 vom 7. April 2003 (=VPB 67.73) zur Berichtigung des Namens eines Asylbewerbers im automatisierten Personenregistratursystem (AUPER 2); die Beschwerde wurde teilweise gutgeheissen.

Im Hinblick auf typische Fallkonstellationen lässt sich demnach auch vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission eine Häufung von Streitigkeiten über Berichtigungsgesuche im Asylbereich, nach Abschluss des Asylverfahrens, feststellen. Daneben gab es vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission einzelne Fälle gestützt auf Art. 25 DSG, die sich auf andere Sachverhalte bezogen:

- Urteil Nr. 2/00 vom 27. Januar 2000 zur Berichtigung durch Vernichtung eines Aktendossiers einer Krankenversicherung; die Beschwerde wurde abgewiesen[31].
- Zum Anspruch auf Vernichtung von Personendaten erging auch das Urteil Nr. 11/01 vom 3. Februar 2003 (= VPB 67.71) zur Akteneinsicht bei der Bundesanwaltschaft; ein Beschwerdeführer verlangte die Vernichtung von Akten, für deren Aufbewahrung keine gesetzliche Grundlage (mehr) existierte; die Beschwerde wurde gutgeheissen.

Auf kantonaler Ebene wurden bezüglich der Durchsetzungsrechte gegen Behördenorgane (kantonale und kommunale Behörden) vorwiegend Berichtigungs- und Vernichtungsansprüche (je sechs Fälle) geltend gemacht. Zum überwiegenden Teil wurden die entsprechenden Ansprüche jedoch abgewiesen[32].

Somit konnte festgestellt werden, dass die überwiegende Mehrzahl der Beschwerden, die gestützt auf Art. 25 DSG vor dem Bundesverwaltungs- und Bundesgericht geltend gemacht wurden, keinen Erfolg hatten. Den Beschwerden wurde nur in seltenen Fällen stattgegeben[33], am ehesten bei Berichtigungsgesuchen.

Die erfolgreichen Berichtigungsersuchen stützten sich auf sehr ähnlich gelagerte Sachverhalte: Einerseits ergab sich eine Häufung von erfolgreichen Berichtigungsgesuchen (und Auskunftsgesuchen[34]) nach abgeschlossenem Asylverfahren. Zahlreichen Berichtigungsfällen im Asylbereich wurde insbesondere von der Eidgenössischen Datenschutz- und Öffentlichkeitskommission stattgegeben.

Eine gewisse Häufung von Ansprüchen aus Art. 25 DSG (5 Fälle vor Bundes- und Bundesverwaltungsgericht) war auch im Bereich der (Sozial-)Versicherungen auszumachen. Die datenschutzrechtlichen Aspekte wurden dabei jedoch regelmässig nicht über die Anspruchsnormen des DSG, sondern nach anderen Verfahren geltend gemacht.

Die dargestellten relativen Häufungen können nichts daran ändern, dass die Durchsetzungsrechte nach Art. 25 DSG selten in Anspruch genommen wurden. Am ehesten in Anspruch genommen und erfolgreich waren Berichtigungsgesuche. Diese stützten sich jedoch in der Hauptsache auf sehr ähnliche, thematisch klar umgrenzte, teils sogar analoge Sachverhaltskonstellationen. Daraus ist zu schliessen, dass sämtliche Ansprüche gestützt auf Art. 25 DSG, die sich ausserhalb jener oben dargestellten Fallgruppen ereignen, praktisch keine Relevanz in der Gerichtspraxis haben.

---

31 Die Verwaltungsgerichtsbeschwerde gestützt darauf wurde mit dem Urteil 1A.6/2001 vom 2. Mai 2001 vom Bundesgericht abgewiesen.

32 Vgl. zu den Berichtigungsgesuchen die Fälle RRB 2.7.91 (AR); ARGVP 1991, 4 ff. (Vernichtung von Polizeiurkunden); Datenberichtigungsbegehren betreffend ein Gemeinderatsprotokoll (OGE SH 60/2004/62, Urteil vom 15. September 2006); Entscheid R 193 der Reko Thurgau vom 9. Juli 1992 und der Entscheid GE.2008.0133 vom 27.10.2008 (Kanton Waadt; beide Aktenvernichtung); Entscheid GE.2006.0208 vom 10.7.2007 (Kanton Waadt, Datenberichtigung betr. ein Polizeirapport). Die angeführten Urteile ergingen nicht gestützt auf das Datenschutzgesetz des Bundes, sondern auf einschlägige kantonale datenschutzrechtliche Bestimmungen. Auf das DSG bzw. auf den Vorentwurf zum DSG wurde jedoch von den kantonalen Behörden als Auslegehilfe für die Interpretation der kantonalen Bestimmungen Bezug genommen.

33 In BGE 122 IV 139 hielt das Bundesgericht nebenbei fest, dass die Ansprüchen im Sinne von Art. 25 Abs. 1-3 DSG in einem Strafverfahren nicht adhäsionsweise geltend gemacht werden können.

34 Dazu oben die Ausführungen zu Art. 8 DSG.

8.4 Gründe für die geringe Inanspruchnahme der Durchsetzungsrechte

Aufgrund der Analyse der Rechtsprechung, der Bevölkerungsbefragung und der Interviewaussagen kann festgehalten werden, dass die Durchsetzungsrechte selten in Anspruch genommen werden. An dieser Stelle soll deshalb möglichen Gründen für diesen Befund nachgegangen werden. Gemäss den Überlegungen zum Wirkungsmodell (vgl. Ziffer 2.2) kann eine tiefe Anzahl Klagen unterschiedlich interpretiert werden. Die optimistische Lesart dieses Befunds ist, dass die seltene Beanspruchung des Gerichtsweges Ausdruck einer hohen Sensibilität der Datenbearbeiter ist, dass also – zugespitzt formuliert – DSG-Bestimmungen in der Praxis gar nicht verletzt werden und somit entweder gar nicht nötig wären oder aber eine präventive Wirkung entfalten. Ist dem so, sind für die Gewährleistung des Datenschutzes keine Rolle, ob die betroffenen Personen in einer solchen Konstellation sensibilisiert sind oder nicht. Die pessimistischere Interpretation der Befunde geht von einer tieferen Sensibilität der Datenbearbeiter aus, was mitunter zur Verletzung der Persönlichkeitsrechte der Betroffenen führt. In diesem Fall ist eine geringe Inanspruchnahme des Rechtsweges Ausdruck einer geringen Sensibilität der Bevölkerung oder möglicherweise weiterer Gründe.

In einem ersten Schritt ist zunächst auf die Sensibilität der Datenbearbeiter einzugehen, wobei wir uns dazu zu einem grossen Teil auf bereits präsentierte empirische Befunde stützen können. Die Ergebnisse der Bevölkerungsbefragung in Bezug auf Missbrauchserfahrungen (vgl. Ziffer 8.2.1), die Einschätzung der Experten hinsichtlich der Einhaltung der DSG-Bestimmungen durch Datenbearbeiter (vgl. Ziffer 4.2) sowie die Analyse der Aufsichtstätigkeit des EDÖB (vgl. Ziffer 12.3) liefern Evidenz dafür, dass es in der Praxis zu Verletzungen der Persönlichkeitsrechte der Betroffenen kommt. Bezüglich des Ausmasses solcher Verstösse kann keine Schätzung gemacht werden; an früherer Stelle hat sich zumindest gezeigt (vgl. Ziffer 4.2), dass es für die Bearbeiter datenschutzbezogene Risiken gibt, die insgesamt zu einer Begrenzung klarer Regelverstösse führen dürften. Insgesamt kann jedoch die These, dass die geringe Inanspruchnahme des Rechtsweges primär der Ausdruck einer hohen Sensibilität aller Datenbearbeiter ist, nicht aufrechterhalten werden.

Somit ist in einem zweiten Schritt bei den Betroffenen selber nach Gründen für die wenigen Klagen zu suchen. Zunächst gilt es zu berücksichtigen, dass den Betroffenen der Datenschutz gemäss der Bevölkerungsbefragung durchaus wichtig ist, so dass sie mehrheitlich ein Interesse an der Wahrung ihrer Persönlichkeitsrechte haben dürften; die Gruppe der Personen, denen die Bearbeitung persönlicher Informationen durch Dritte egal ist, ist relativ klein.

Lücken zeigen sich dagegen bei den Kenntnissen der Durchsetzungsrechte bzw. beim Wissen, wie diese anzuwenden sind: Gemäss der Bevölkerungsbefragung ist sich nur jede und jeder vierte sicher, dass er bei einer Datenschutzverletzung vor Gericht gehen kann und es gibt Hinweise, dass der Begriff des Datenmissbrauchs in der Bevölkerung eher diffus ist und nicht unbedingt mit demjenigen des DSG übereinstimmt. Darüber hinaus vermuten die befragten Experten eine Überforderung der Betroffenen bei der konkreten Anwendung der rechtlichen Möglichkeiten, da diese einiges an juristischem Sachverstand erfordert. Schliesslich räumt ein bedeutender Teil der Betroffenen in der Umfrage selbst ein, beim Selbstschutz nicht immer konsequent zu sein.

Die festzustellende Diskrepanz zwischen Bewusstsein (Datenschutz wird als wichtig erachtet) und Verhalten (man tut eher wenig für den Schutz der eigenen Daten) zumindest bei einem Teil der Bevölkerung erscheint auch in Bezug auf die Inanspruchnahme des Gerichtswegs plausibel, wenn man sich mögliche Kosten- und Nutzenüberlegungen eines Betroffenen im Missbrauchsfall vor Augen führt. In verschiedenen Interviews wurde deutlich gemacht, dass der Nutzen, der sogar bei einer erfolgreichen Inanspruchnahme der Durchsetzungsrechte resultieren kann, in aller Regel als gering eingestuft wird, so dass der Aufwand und das Risiko, den Rechtsweg zu beschreiten, selbst bei dessen Kenntnis sich nicht lohnen würde. Neben der zeitlichen und finanziellen Beanspruchung durch einen Prozess sind auch die Erfolgsaussichten zu berücksichtigen; wie die Analyse der Rechtsprechung zeigt, ist die Erfolgswahrscheinlichkeit nicht sehr hoch. Zudem ist es kaum möglich, den entstandenen Schaden eines Missbrauchs zu quantifizieren oder abzuschätzen, welche weiteren Folgen sich aus einer Datenschutzverletzung ergeben können. Von einem Interessenvertreter wird ausserdem erwähnt, dass im Arbeitsbereich das Beschreiten des Rechtswegs mit hohen Risiken verbunden sei und im schlimmsten Fall zu einer Kündigung führen könne, was zu einer sehr zurückhaltenden Inanspruchnahme der Rechte führe.

Schliesslich gilt es auf einen Umstand hinzuweisen, der sich im Zuge der technologischen Herausforderungen ergibt (vgl. Kapitel 3): Datenbearbeitungen sind aufgrund der verfügbaren technischen Möglichkeiten verschiedentlich für die Betroffenen nicht mehr erkennbar. Die Frage nach den Missbrauchserfahrungen in der Bevölkerung lässt vermuten, dass es sich häufig um eher klassische Situationen handelt, wenn Betroffene einen Missbrauch vermuten. In die gleiche Richtung deutet auch die qualitative Analyse der Gerichtsurteile im folgenden Kapitel. Somit muss zumindest berücksichtigt werden, dass ein Teil von Persönlichkeitsverletzungen für die Betroffenen – selbst wenn sie sehr sensibilisiert sind – gar nicht erkennbar ist. Dieses Argument lässt sich grundsätzlich auch für klassische Konstellationen anführen, es dürfte aber angesichts des technischen Wandels zunehmend an Bedeutung gewinnen.

9 Anwendung und Konkretisierung des DSG durch die Gerichte

Die qualitative Betrachtung der Rechtsprechung soll der Frage nachgehen, welche materiell- oder prozessrechtlichen Bestimmungen oder Argumente der erfolgreichen Geltendmachung des Auskunftsrechts und der Durchsetzungsrechte entgegenstehen könnten (z.B. Rechtfertigungsgründe oder gesetzliche Ausnahmen zur Zulässigkeit der Datenbearbeitung) und wie diese Gegenargumente von den rechtsanwendenden Behörden ausgelegt werden. Ergänzend wird kurz auf die Anwendung der Strafbestimmungen vor Gericht eingegangen.

Die Analyse der Gerichtsurteile wird jeweils mit einem Überblick zum Inhalt des betreffenden Durchsetzungsrechts eingeleitet, der so weit gehen soll, wie es für das Verständnis und die Analyse der Rechtsprechung und allfällige Empfehlungen auf Gesetzesstufe erforderlich ist. Die Erkenntnisse aus der qualitativen Betrachtung sind schliesslich jeweils am Ende des Abschnitts im Sinne eines Fazits kurz zusammenzufassen und zu würdigen, um am Ende des Gesamtkapitels Schlussfolgerungen zu formulieren.

9.1 Akteneinsicht (Art. 8 DSG)

9.1.1 Inhalt des Einsichtsrechts

Das Recht auf Akteneinsicht findet sich in den allgemeinen Bestimmungen des DSG (Art. 8 DSG). Dieses Recht räumt jeder urteilsfähigen Person, unabhängig von deren Nationalität, das Recht ein, Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen. Dieses Recht kann jederzeit geltend gemacht werden; der Nachweis eines persönlichen Interesses ist nicht erforderlich.

Das Auskunftsrecht ist von herausragender Bedeutung in der Praxis der Gerichte; es wird wesentlich häufiger angerufen als die Durchsetzungsrechte wie sie in Art. 15 DSG für die Datenbearbeitung durch Private, in Art. 25 für die Datenbearbeitung durch Bundesorgane und gemäss Art. 27 bzw. 29 DSG für die Beschwerdebefugnis des EDÖB festgelegt sind. Das Auskunftsrecht ist ein zentrales Element des Datenschutzes und eine unerlässliche Voraussetzung für die Ausübung der Durchsetzungsrechte. Nur wenn eine betroffene Person erfahren kann, wer über sie Daten bearbeitet, ist sie in der Lage, gegen eine unzulässige Datenbearbeitung vorzugehen.

Das Auskunftsrecht ist ein jeder Person voraussetzungslos zustehendes höchstpersönliches Recht. Es kann nicht für Dritte ausgeübt werden, ist weder übertragbar noch vererblich[35], auch

[35] Vgl. aber Art. 1 Abs. 7 VDSG: Betrifft die Auskunft eine verstorbene Person, ist sie nur unter den Voraussetzungen von Art. 1 Abs. 7 VDSG zu erteilen. Namentlich muss ein tatsächliches Interesse an der Auskunft nachgewiesen werden, und es dürfen ihr keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder Dritten entgegenstehen. Nahe Verwandtschaft begründet ein Interesse, vgl. dazu auch Rosenthal, Rz. 13 zu Art. 8. In einem Entscheid des Regierungsrates des Kantons Aargau vom 20.11.2002 i.S. M. und S. sowie M.M. gegen das Gesundheitsdepartement war für eine über das für einen Arzthaftungsprozess erforderliche Material hinausgehende Einsicht in die Krankengeschichte allerdings auch von nahen Verwandten ein Interessensnachweis nötig; dem Antrag der Angehörigen auf Akteneinsicht wurde nur teilweise stattgegeben.

ist es keiner zeitlichen Einschränkung unterworfen[36]. Des Weiteren ist der vorgängige Verzicht auf das Auskunftsrecht nicht möglich[37]; eine entsprechende Verzichtserklärung wäre nichtig.

Verantwortlich für die Herausgabe der Information gestützt auf das Auskunftsrecht im Sinne von Art. 8 DSG ist der Inhaber der Datensammlung. Dies gilt auch, wenn er die Datensammlung durch eine Drittperson bearbeiten lässt[38]. Dabei trifft den Dritten auch eine Auskunftspflicht sofern er entweder den Inhaber nicht bekannt gibt oder der Inhaber keinen Wohnsitz in der Schweiz hat[39].

Hat eine Datensammlung mehrere Inhaber, ist jeder zur Auskunft verpflichtet, es sei denn, es bestehe eine klare interne Rollenverteilung, die auch nach aussen bekannt gegeben wird[40].

Das Recht auf Auskunft gemäss Art. 8 DSG umfasst auch das Anrecht auf Zugang zu Informationen, die sich auf die Person des Betroffen selbst beziehen.

Das Auskunftsrecht ist umfassend: Eine betroffene Person kann über alle zu ihr in der betreffenden Datensammlung vorhandenen Daten Auskunft verlangen; ebenso kann sie Auskunft darüber verlangen, woher diese Daten stammen, sofern dies möglich ist[41]. Der betroffenen Person sind sämtliche Informationen zum Zwecke der Bearbeitung und deren Rechtsgrundlagen zu eröffnen. Die Kategorie der bearbeiteten Daten ist zu nennen, ebenso wie die an der Datenbearbeitung Beteiligten, insbesondere die Datenempfänger, d.h. die Personen und Stellen, an welche die Daten übermittelt werden[42].

Hinsichtlich der Anforderungen an den Antrag der Betroffenen ist folgendes festzuhalten:

- Der Auskunftsantrag muss in der Regel schriftlich verfasst werden; der Gesuchsteller muss seine Identität belegen[43]. In der Regel wird die Auskunft in Form eines Auszugs oder einer Kopie aus der Datensammlung erteilt[44].
- Sowohl das Auskunftsbegehren als auch die Auskunftserteilung können grundsätzlich auch auf elektronischem Weg erfolgen, sofern die Identifizierung der antragstellenden Person sowie die Sicherheit der Daten gewährleistet ist[45].
- Ausnahmsweise können auf Vorschlag oder mit dem Einverständnis des Inhabers der Datensammlung die Daten an Ort und Stelle eingesehen werden[46]; selbstverständlich muss der

36 VPB 62.38.
37 Art. 8 Abs. 6 DSG.
38 Art. 8 Abs. 4 Satz 1 DSG.
39 Art. 8 Abs. 4 Satz 2 DSG.
40 Art. 1 Abs. 5 VDSG. Um in der Praxis das Risiko zu vermeiden, dass Auskunftsbegehren aufgrund mangelhafter Organisation nicht oder nicht rechtzeitig behandelt werden, empfiehlt es sich, die internen Verantwortlichkeiten nicht nur festzulegen, sondern auch intern und extern zu kommunizieren, z.B. mittels Kontaktinformationen auf Websites.
41 Vielleicht wäre hier der Begriff zumutbar besser als „verfügbar“, wie er in Art. 8 Abs. 2 Bst. a DSG festgehalten wird.
42 Art. 8 Abs. 2 DSG.
43 Art. 1 Abs. 1 VDSG.
44 Art. 8 Abs. 5 DSG.
45 Art. 1 Abs. 2 VDSG.
46 Art. 1 Abs. 3 VDSG.

Betroffene mit dieser Vorgehensweise einverstanden sein[47]. Auch eine mündliche Auskunft ist möglich, wenn die betroffene Person vorab eingewilligt hat[48].

- Die Auskunft – oder der begründete Entscheid über die Beschränkung des Auskunftsrechts – muss innerhalb von 30 Tagen ab Eingang des Auskunftsbegehrens erteilt werden[49].
- In der Regel erfolgt die Auskunft kostenlos[50]. Ausnahmsweise kann jedoch eine Kostenbeteiligung in der Höhe von maximal 300 CHF erhoben werden[51], falls die betroffene Person in den letzten zwölf Monaten die gewünschten Auskünfte bereits erhalten hat[52]. Eine solche Kostenbeteiligung kann auch erhoben werden, wenn die Auskunftserteilung einen besonders grossen Arbeitsaufwand verursacht[53], beispielsweise wenn langwierige Nachforschungen notwendig sind[54].
- Auf Verlangen des Gesuchstellers muss eine Kostenbeteiligung in Form einer selbständig anfechtbaren Zwischenverfügung festgesetzt werden. Die Erhebung einer Kostenbeteiligung setzt einen über das blosse Kopieren und Versenden der Akten hinausgehenden Aufwand voraus[55]. Die Erhebung einer Kostenbeteiligung ist dann nicht zulässig, wenn der Gesuchsteller die Voraussetzungen der unentgeltlichen Rechtspflege erfüllt[56].

Ausnahmsweise, und nur aufgrund der in Art. 9 und 10 DSG abschliessend aufgeführten Voraussetzungen, kann das Recht auf Auskunft verweigert, eingeschränkt oder aufgeschoben werden. Dies ist einerseits der Fall, wenn ein Gesetz im formellen Sinne dies vorsieht[57] oder wenn dies aufgrund überwiegender Interessen Dritter erforderlich ist[58].

Ein Bundesorgan kann zudem die Auskunft verweigern, einschränken oder aufschieben, wenn dies wegen überwiegender öffentlicher Interessen – insbesondere der inneren oder äusseren Sicherheit – erforderlich ist, oder wenn die Auskunft den Zweck einer Strafuntersuchung oder eines andern Untersuchungsverfahrens in Frage stellt[59].

Geht es um die Einschränkung des Auskunftsrechts aufgrund überwiegender Interessen Dritter oder aufgrund überwiegender öffentlicher Interessen, ist die Abwägung zwischen den Interessen der um Auskunft ersuchenden Person und den Interessen des Dritten bzw. den öffentlichen In-

---

47 BGE 125 II 321.
48 Art. 1 Abs. 3 VDSG.
49 Zumindest muss der Inhaber der Datensammlung die Frist mitteilen, innerhalb welcher die Auskunft erfolgen wird; Art. 1 Abs. 4 VDSG.
50 Art. 8 Abs. 5 DSG.
51 Art. 2 Abs. 2 VDSG.
52 Falls sich die betroffene Person jedoch auf ein schutzwürdiges Interesse berufen kann, z.B. auf eine Änderung der Daten in der Zwischenzeit, darf trotzdem keine Gebühr verlangt werden; Art. 2 Abs. 1 Bst. a VDSG.
53 Art. 2 VDSG.
54 Vgl. dazu VPB 64.72. Den Behörden steht hier ein gewisser Ermessensspielraum zu; die Festlegung der Gebühr muss aber mit Blick auf die vom Verordnungsgeber vorgegebene Maximalgebühr von CHF 300.- angemessen sein. die Angemessenheit der Kostenbeteiligung einerseits nach dem Aufwand der datenbearbeitenden Stelle und andererseits nach dem persönlichkeitsverletzenden Potential der gespeicherten Daten im Einzelfall; Urteil des Präsidenten der Eidgenössischen Datenschutzkommission vom 15. März 1999; VPB 64.72.
55 Dies vorbehältlich eines ausserordentlich grossen Aktenumfanges; VPB 65.50.
56 Vgl. VPB 65.49.
57 Art. 9 Abs. 1 Bst. a DSG.
58 Art. 9 Abs. 1 Bst. a DSG.
59 Art. 9 Abs. 2 DSG.

teressen besonders wichtig. Denn es ist das Ergebnis dieser Abwägung, das für die Gewährung des Einsichtsrechts oder dessen Verweigerung entscheidend ist. Auch bei dieser Abwägung ist zu beachten, dass das Auskunftsrecht die Regel, seine Einschränkung jedoch die Ausnahme darstellt.

Ganz allgemein ist bei der Entscheidung über die Gewährung des Einsichtsrechts der Grundsatz der Verhältnismässigkeit zu beachten. Daher stellt der Umstand, dass ein Datenträger Daten verschiedener Personen enthält, für sich alleine keinen Verweigerungsgrund des Auskunftsrechts dar. Vielmehr ist der Datenträger in geeigneter Weise zu behandeln, um das Auskunftsrecht ohne Verletzung des Amtsgeheimnisses und berechtigter Datenschutzinteressen von Drittpersonen zu gewährleisten[60].

Dabei ist hervorzuheben, dass nicht jedes öffentliche Interesse als überwiegend im Sinne von Art. 9 Abs. 2 DSG zu gelten hat. Z.B. der mit der Einsicht verbundene Aufwand, d.h. die Effizienz der Verwaltungsabläufe oder auch politische Interessen begründen kein überwiegendes öffentliches Interesse. Insbesondere kann der Verweigerungsgrund des überwiegenden öffentlichen Interesses i.S.v. Art. 9 Abs. 2 Bst. a DSG nicht pauschal für bestimmte Kategorien von Auskunftsersuchen geltend gemacht werden, sondern muss im Einzelfall, mit Bezug auf diejenigen Akten, für welche die Einsicht verweigert werden soll, konkret geprüft werden.

Bei einem Straf- oder einem anderen Untersuchungsverfahren gemäss Art. 9 Abs. 2 Bst. b DSG ist eine Einschränkung nicht schon dann zulässig, wenn bloss die ferne Möglichkeit der Infragestellung des Untersuchungszwecks besteht, sondern nur dann, wenn sich diese Möglichkeit als sehr wahrscheinlich erweist.

Der Inhaber der Datensammlung ist verpflichtet anzugeben, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen er die Auskunft verweigert, einschränkt oder aufschiebt[61].

9.1.2 Qualitative Analyse

Die charakteristischen Fälle zum Auskunftsrecht nach Art. 8 DSG betrafen vor dem Bundes- bzw. dem Bundesverwaltungsgericht vor allem die Bereiche Hochschule, Versicherung und Asyl[62].

Im Folgenden sollen aus jenen drei Bereichen typische Fälle zum Auskunftsrecht, die vor die Gerichte gebracht wurden, herausgegriffen, in ihren typischen Elementen gewürdigt und zusammengefasst werden.

Bereiche Hochschule und Sicherheit

In einem ersten Fall zum Bereich Auskunftsrecht und Hochschulen hatte das Bundesgericht Fragen zur Zulässigkeit der Herausgabe von Daten zu behandeln.

60 VPB 62.55.
61 Art. 9 Abs. 4 DSG.
62 Daneben bildeten auch Themen wie SBB, EDA/Rechtshilfe oder Bonus-Zahlungen Gegenstand von Verfahren.

Der Beschwerdeführer war als Leiter der Informatikabteilung der Universität Genf angestellt. Letztere beauftragte einen externen Psychologen mit der Begutachtung des Beschwerdeführers. Der Psychologe händigte der Universität zwei Berichte über den Beschwerdeführer aus, die besagten, dass er für seine Stelle nicht geeignet sei. Der Beschwerdeführer, der die Universität Genf unterdessen verlassen hatte, verlangte die Herausgabe aller Berichte über ihn, was vom zuständigen kantonalen Gericht verweigert wurde.

Das angerufene Bundesgericht hielt zunächst fest, dass es sich vorliegend um Personendaten[63] und um eine Bearbeitung durch eine private Person handle[64]. Weiter führte es aus, dass gemäss Art. 8 DSG jede Person vom Inhaber einer Datensammlung Auskunft über die über ihn bearbeiteten Daten verlangen könne; insbesondere könne jede Person von ihrem Arzt oder Psychologen Auskunft über die sie betreffenden Daten anfordern. Neben den Ausnahmen von Art. 9[65] schliesse das DSG vom Einsichtsrecht grundsätzlich Personendaten aus, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeite und nicht an Aussenstehende bekannt gebe[66]. Als solche würden insbesondere der Inhalt einer Agenda, Gespräche im Familien- oder Freundeskreis, Privatkorrespondenz oder Handnotizen gelten, die man bei der Ausübung seines Berufs als Gedankenstütze erstelle – solange man sie nur zum persönlichen Gebrauch benütze. Diese Ausnahmebestimmung zum persönlichen Gebrauch müsse jedoch sehr vorsichtig und eng ausgelegt werden; das Auskunftsrecht dürfe nur soweit als wirklich nötig eingeschränkt werden.

Der beigezogene Psychologe hatte die Daten der Universität zur Verfügung gestellt; sie wurden weitergeleitet – und damit nicht ausschliesslich zum persönlichen Gebrauch[67] verwendet. Die Ausnahme im Sinne von Art. 2 Abs. 2 Bst. a DSG konnte nicht mehr greifen. Entsprechend konnte der Beschwerdeführer sein Auskunftsrecht gemäss Art. 8 DSG geltend machen und – unter den Einschränkungen von Art. 9 DSG – die Mitteilung aller ihn betreffenden Daten verlangen, die sich in der fraglichen Datensammlung befunden hatten[68]. Das Bundesgericht ordnete an, dass der von der Universität Genf beigezogene Psychologe dem Beschwerdeführer Kopien von sämtlichen ihn betreffenden Dokumenten, die er der Universität übermittelt hatte, herausgeben musste[69].

Das Gericht legte somit die Ausnahmebestimmung des persönlichen Gebrauchs, die eine Datenbearbeitung erlauben würde, zu Recht eng aus. Wenn das Vorliegen der Ausnahmebestimmung des persönlichen Gebrauchs in Fällen wie diesem bejaht würde, käme dies einem Rechtsmissbrauch gleich[70].

---

63 Art. 3 Bst. a DSG.

64 Der beigezogene Psychologe – ein Privater im Sinne von Art. 2 Abs. 1 Bst. a DSG – hatte die Daten im Rahmen seines Mandats gesammelt und damit bearbeitet; Art. 3 Bst. e DSG.

65 D.h. wenn eine gesetzliche Grundlage eine Einschränkung dies vorsieht oder wegen überwiegender Interessen Dritter; vgl. Ziffer 9.1.1.

66 Art. 2 Abs. 2 Bst. a DSG.

67 Im Sinne von Art. 2 Abs. 2 Bst. a DSG.

68 Art. 8 Abs. 2 Bst. a DSG.

69 Die Namen der befragten Mitarbeiter durften jedoch abgedeckt werden; BGer 5C.15/2001 (vgl. auch 5C.242/2003); Urteil vom 16. August 2001.

70 So auch das Bundesgericht explizit in seinem Entscheid.

In einem weiteren Verfahren wurde das Recht auf Einsichtnahme in persönliche Akten von der Einsichtnahme in Daten Dritter abgegrenzt. Vor dem Bundesverwaltungsgericht verlangte ein von der Ecole Polytechnique Fédérale in Lausanne (EPFL) definitiv abgewiesener Student Zugang zu seinen persönlichen Daten. Während des Verfahrens erhielt der Beschwerdeführer Zugang zu seinem Dossier; insofern er aber beantragte, auch Daten einer Vereinigung einzusehen, deren Mitglied er damals war, konnte ihm kein Einsichtsrecht gewährt werden: Eine Einsichtnahme gestützt auf Art. 8 DSG lassen die Gerichte immer nur dann zu, wenn eigene Daten eingesehen werden sollen. Das Einsehen von Daten zu Drittpersonen kann nicht mit dem Einsichtsrecht nach Art. 8 DSG geltend gemacht werden[71].

In Anbetracht der Rüge des abgewiesenen Studenten, das ihm übermittelte Dossier sei unvollständig, nahm das Gericht auch Stellung zur Frage, inwiefern bezüglich weiterer Aktenstücke vorzugehen ist, deren Vorhandensein lediglich behauptet wird (unvollständige Akteneinsicht). Und hier sind die Gerichte streng: die blosse Behauptung des Vorliegens von weiteren Aktenstücken ohne Beweis für deren Vorhandensein reiche für ein Recht auf Einsicht in entsprechende Aktenstücke nicht aus; das Vorliegen weiterer Aktenstücke sei glaubhaft zu machen[72].

In einem weiteren Fall zum Hochschulbereich stellte sich vor dem Bundesgericht die Frage, wie weit das Einsichtsrecht in Bezug auf sog. interne Akten reichen würde. Diesbezüglich wurde festgehalten, dass im Hinblick auf einen allfälligen Rekurs die Verweigerung der Einsicht in interne Korrekturtabellen, Notizen und Bemerkungen der Prüfer von Universitätsprüfungen nicht gegen Prozessrechte wie das rechtliche Gehör oder gegen Art. 8 und 9 des Datenschutzgesetzes verstosse. Solche internen Akten seien zur internen Meinungsbildung erforderlich und könnten von den Studierenden und Dritten nicht eingesehen werden. Dagegen seien die Dokumente, die direkt die Prüfungsfragen und die Antworten des Prüfungskandidaten betreffen, wie auch die Bewertung der Prüfenden Grundlagen für die Note und müssten eingesehen werden können[73].

Diese Argumentation überzeugt insofern nicht, als auch interne Korrekturtabellen für die Benotung des betreffenden Kandidaten entscheidend sein können. Zumindest bilden sie eine Grundlage für die Bewertung des Prüfungskandidaten und sollten daher eingesehen werden können. Allgemein ist festzuhalten, dass das Recht der Einsichtnahme in persönliche Daten stark eingeschränkt werden kann, wenn sich in der Gerichtspraxis Fallgruppen von sog. internen Akten herausbilden. Das Recht auf Akteneinsicht darf jedenfalls durch die Bildung von internen Akten nicht eingeschränkt werden (dazu ausführlicher unten).

In einem weiteren Urteil vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission[74] zum Auskunftsanspruch nach Art. 8 DSG beantragte ein Beschwerdeführer bei der Oberzolldirektion Auskunft bezüglich aller über ihn gespeicherter Daten. Laut Angaben der Oberzolldirektion waren jedoch keine entsprechenden Daten gespeichert. Die Rekurskommission führte aus, das DSG setze voraus, dass die vom Inhaber einer Datensammlung zu erteilende Auskunft der

71 A-7373/2006, E. 3.2, Urteil vom 13. Februar 2008. Vgl. z.B. auch VPB 67.70, E. 2.
72 A-7373/2006, E. 4.4 f., Urteil vom 13. Februar 2008.
73 1P.742/1999, Urteil vom 15. Februar 2000.
74 Urteil Nr. 8/99 vom 8. Dezember 2000 (=VPB 67.70).

Wahrheit entspreche. Dafür, dass der Inhaber einer Datensammlung wahrheitsgemäss Auskunft erteilt habe, sei er im Streitfall auch beweispflichtig.

Wiederholt wurde jedoch gleichermassen auch der Grundsatz, dass die blosse Behauptung des Beschwerdeführers, die ihm erteilte Auskunft sei unvollständig oder unwahr – wie bereits für den Bereich Hochschulfälle ausgeführt –, für sich allein keine Grundlage dafür bieten könne, dass dies tatsächlich so sei. Der Beschwerdeführer hatte im vorliegend angesprochenen Urteil der Eidgenössischen Datenschutz- und Öffentlichkeitskommission trotz mehrfacher Aufforderung der EDSK nicht mitgeteilt, woraus er den Verdacht ableitete, dass seine persönlichen Daten entgegen der ihm erteilten Auskunft bearbeitet würden. Er hatte auch nicht angegeben, an welchen Zollstellen er angeblich Schwierigkeiten hatte, sodass das Gericht dort ergänzende Abklärungen hätte vornehmen können. In solchen Fällen können demnach die Gerichte auf die Beschwerde nicht eintreten.

Bereich Versicherungen

Die Gerichte äusserten sich auch zu Fragen zur Abgrenzung datenschutzrechtlicher Verfahren gegenüber anderen Ansprüchen. Eine Versicherte verlangte bei ihrer Unfallversicherung Einsicht in sämtliche Unterlagen bezüglich eines Schadenereignisses. Die Versicherung weigerte sich jedoch, diese Einsicht in der Form zugesandter Kopien zu gewähren. Dagegen erhob die Versicherte Beschwerde. Die Eidgenössische Datenschutz- und Öffentlichkeitskommission hiess die Beschwerde gut. Gegen diesen Entscheid erhob die Versicherung damals Verwaltungsgerichtsbeschwerde ans Bundesgericht, welches die Beschwerde abwies[75] und dabei zunächst allgemein festhielt, dass das datenschutzrechtliche Auskunftsrecht gemäss Art. 8 DSG nur teilweise mit dem verfahrensrechtlichen Akteneinsichtsrecht gemäss UVG übereinstimme. Insoweit Art. 8 DSG eine eigenständige Bedeutung habe, die von konkreten unfallversicherungsrechtlichen Leistungsansprüchen unabhängig ist, seien Streitigkeiten darüber nicht im Verfahren nach Art. 105 ff. UVG, sondern im datenschutzrechtlich vorgesehenen Verfahren zu entscheiden. Es handle sich um einen datenschutzrechtlichen Anspruch und hieraus ergebe sich die Zuständigkeit der Datenschutzkommission und auch des Bundesgerichts. Ein separates Verfahren nach dem Datenschutzgesetz mit den entsprechenden Schutzrechten einzuleiten, sei jedenfalls immer dann möglich, wenn das Auskunftsbegehren unabhängig von einer konkreten unfallversicherungsrechtlichen Streitigkeit gestellt werde[76].

Für das konkrete Verfahren hiess dies, dass sich die Modalitäten des Akteneinsichtsrechts nach den Bestimmungen des Datenschutzgesetzes richteten[77]. Die Beschwerdeführerin war hinsichtlich ihrer Tätigkeit als UVG-Versicherer ein Bundesorgan im Sinne von Art. 3 Bst. h DSG. Sie habe daher gemäss Art. 8 Abs. 5 DSG in der Regel schriftlich[78], in Form eines Ausdrucks oder einer Fotokopie, Auskunft zu erteilen. Die Zustellung der Fotokopien zu verweigern – so das

[75] BGE 123 II 534.
[76] BGE 123 II 534.
[77] Art. 8-10 DSG, Art. 1 und 2 VDSG.

Bundesgericht –, wäre eine mit dem Gesetz unvereinbare Erschwerung des Auskunftsrechts gewesen. Damit war die versicherte Privatperson durch das weiter gehende Einsichtsrecht nach dem datenschutzrechtlichen Verfahren geschützt.

In einem weiteren, ähnlich gelagerten Fall ersuchte der Beschwerdeführer seine Krankenkasse für die Abklärung von Demarchen um Kopien seines medizinischen Dossiers. Die Krankenkasse verweigerte die Herausgabe mit der Begründung, dass die entsprechenden Briefe bereits in seinem Besitz seien; das Dossier könne am Hauptsitz der Krankenkasse eingesehen werden. Die Eidgenössische Datenschutzkommission hiess die darauf gestützte Beschwerde gut. Gegen diesen Entscheid erhob die Versicherung Verwaltungsgerichtsbeschwerde beim Bundesgericht, welches die Beschwerde abwies[79].

Das Bundesgericht hielt fest, dass ein Krankenkassendossier Personendaten im Sinne von Art. 3 Bst. a DSG enthielten. Das Auskunftsrecht richte sich deshalb nach Art. 8 und 9 DSG. Gemäss Art. 8 Abs. 5 DSG[80] hat die Auskunft in der Regel schriftlich zu erfolgen, daher habe die Krankenkasse dem Versicherten entsprechende Kopien zuzustellen.

In einem weiteren Fall zum Einsichtsrecht im Versicherungsbereich hatte das Bundesgericht zu beurteilen, inwiefern die Weigerung einer IV-Stelle, einem Versicherten Kopien eines Gutachtens einer Medizinischen Abklärungsstelle zuzusenden, gerechtfertigt war[81]. Das Bundesgericht stellte zunächst fest, dass der Anspruch eines Versicherten auf Akteneinsicht im Sinne von Art. 8 des Datenschutzgesetzes dem Betroffenen auch in einem sozialversicherungsrechtlichen Verfahren zustehe. Die Weigerung der IV-Stelle, dem Beschwerdeführer eine Kopie des Gutachtens der Medizinischen Abklärungsstelle zuzustellen, sei damit mit den Ansprüchen des Versicherten hinsichtlich der Bekanntgabe persönlicher Daten im Sozialversicherungsbereich nicht vereinbar. Auch die IV-Stelle hatte dem Versicherten demnach Kopien auszustellen.

Des Weiteren hatte das Bundesgericht bezüglich der Einschränkung des datenschutzrechtlichen Auskunftsrechts nach Art. 9 DSG Stellung zu nehmen. Ein Beschwerdeführer erlitt einen Unfall, als Folge dessen er bei der SUVA Versicherungsleistungen beanspruchte. Er verlangte die Herausgabe seiner sämtlichen persönlichen Unterlagen, die er dann aber als unvollständig beurteilte. Die SUVA teilte mit, dass weitere interne Akten nicht herausgegeben werden könnten. Die daraufhin erhobene Beschwerde wies die Eidgenössische Datenschutzkommission ab. Die vom Betroffenen gegen diesen Entscheid erhobene Verwaltungsgerichtsbeschwerde hiess das Bundesgericht gut[82].

Das Bundesgericht hatte sich zunächst mit der Frage auseinanderzusetzen, inwiefern das datenschutzrechtliche Einsichtsrecht gegenüber dem verfahrensrechtlichen Akteneinsichtsrecht abzugrenzen sei. Auch hier wurde wiederum festgehalten, dass das datenschutzrechtliche Auskunftsrecht und das verfahrensrechtliche Akteneinsichtsrecht selbständige Ansprüche seien, von denen

---

78 Nur das Einverständnis des Betroffenen oder aber eine Art von Daten, über die eine schriftliche Auskunftserteilung nicht möglich ist (z.B. Ton- und Filmaufnahmen) lassen eine Abweichung vom Grundsatz der Schriftlichkeit zu; Maurer-Lambrou/Vogt, N. 48 zu Art. 8 und oben.

79 BGE 125 II 321.

80 Zu beachten waren auch Art. 1 und 2 VDSG.

81 BGE 127 V 219.

82 BGE 125 II 473.

jeder seinen eigenen Anwendungsbereich hätten. Die Ausnahmen vom datenschutzrechtlichen Auskunftsrecht seien in den Art. 9 und 10 DSG *abschliessend* normiert. Diese Ausnahmen könnten nicht zusätzlich, gestützt auf Bestimmungen zum allgemeinen verfahrensrechtlichen Akteneinsichtsrecht eingeschränkt werden.

Mit Bezug auf die bereits thematisierten sog. internen Akten wurde ausgeführt, dass für diese kein verfassungsmässiger Anspruch auf Einsicht bestehe[83]. Als verwaltungsinterne Akten bezeichnete das Bundesgericht jene Akten, denen für die Behandlung eines Falles keine Beweiskraft zukomme, sondern die vielmehr ausschliesslich der verwaltungsinternen Meinungsbildung dienten (z.B. Entwürfe, Anträge, Notizen, Mitberichte, Hilfsbelege usw.). Mit dem Ausschluss des Einsichtsrechts in die internen Akten solle – so das Bundesgericht – verhindert werden, dass die interne Meinungsbildung der Verwaltung über die entscheidenden Aktenstücke und die erlassenen Verfügungen hinaus vollständig vor der Öffentlichkeit ausgebreitet werde. Gleichermassen hielt das Bundesgericht jedoch fest, dass sich der Auskunftsanspruch gemäss Art. 8 DSG auch auf Akten erstrecke, die zwar von der Verwaltung als „intern" bezeichnet werden, die aber Angaben über den Gesuchsteller enthalten und diesem zugeordnet werden können.

Das Bundesgericht begründete seine Argumentation mit dem Hinweis, dass erst das Auskunftsrecht den Betroffenen in die Lage versetze, seine übrigen Datenschutzrechte wahrnehmen zu können. Das Auskunftsrecht ermögliche es dem Betroffenen, auch die Einhaltung der materiellen Grundsätze des Datenschutzes zu überprüfen und seine Rechte wahrzunehmen, so z.B. die Berichtigung unrichtiger Daten[84] die Sperrung der Bekanntgabe gewisser Daten[85] oder die Anonymisierung und Vernichtung nicht benötigter Daten zu verlangen[86]. Diese Rechte müsse der Betroffene gerade auch bezüglich interner, ihm im Verwaltungsverfahren nicht ohne Weiteres zugänglicher Akten ausüben können, namentlich wenn diese - wie die internen Akten der SUVA - besonders schützenswerte Personendaten enthalten (z.B. über medizinische Befunde). Die Bezeichnung der Akten als intern kann damit die Tragweite des Auskunftsrechts nicht grundlegend modifizieren.

Es fragte sich damit im vorliegenden Fall einzig, ob Gründe vorlagen, die eine Einschränkung des datenschutzrechtlichen Auskunftsrechts nach Art. 9 DSG rechtfertigen konnten. Dies wurde für die internen Aufzeichnungen in einem hängigen erstinstanzlichen Verfahren bejaht. Die Einschränkung des Einsichtsrechts müsse jedoch auf das zeitlich und sachlich unbedingt Notwendige begrenzt werden. Unter datenschutzrechtlichen Gesichtspunkten sei dabei ausschliesslich die Art und der Inhalt eines Dokuments von Bedeutung und nicht seine Entscheidrelevanz und Klassifikation als interne Akte durch die SUVA. Es war demnach im Einzelnen zu prüfen, ob die Bekanntgabe eines Dokumentes während des hängigen erstinstanzlichen Verfahrens dessen Ab-

83 Damals Art. 4 aBV.
84 Art. 5 Abs. 2 DSG,
85 Art. 20 Abs. 1 DSG.
86 Art. 21 DSG. Die Möglichkeit zur Überprüfung besteht auch für weitere Grundsätze wie Zweckbindung und das Verbot der Vorratsdatenspeicherung: Gemäss Art. 4 DSG muss die Bearbeitung von Personendaten verhältnismässig sein (Abs. 2) und sie darf nur zum Zweck erfolgen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Abs. 3). Das Datenschutzgesetz verbietet daher das Sammeln von Personendaten «auf Vorrat» und verlangt, dass nur diejenigen Daten erhoben und gespeichert werden, die eine Behörde zur Erfüllung ihrer Aufgabe objektiv benötigt.

lauf gefährde und ob das öffentliche Geheimhaltungsinteresse das private Interesse auf Information überwiege.

Bereich Asyl

In einem Urteil vor Bundesverwaltungsgericht stand die Interessenabwägung zur Einschränkung des Einsichtsrechts zur Entscheidung und es stellten sich Fragen zum Begründungserfordernis und zum Ermessen beim Einsichtsrecht von Akten[87].

Bei einem Asylsuchenden aus dem ehemaligen Jugoslawien hatte das Bundesamt für Migration[88] beim Eintrag über die Staatsangehörigkeit im AUPER2-Register „kroatisch" mit dem Zusatz „unbekannt" eingetragen. Der Asylsuchende beantragte, dass die Nationalität „Sozialistische Föderative Republik Jugoslawien" eingetragen werde. Weiter verlangte der Beschwerdeführer, dass alle Akten, welche sich widerrechtlich beim BFM befänden, zu löschen seien, und dass das BFM die persönlichen Daten nicht an Drittstaaten bzw. Drittpersonen weitergebe. Zudem wurde die vollständige Einsicht in alle verwehrten Akten beantragt.

Das Gericht führte dazu aus, das wenn immer eine Ausnahme zur Nichtgewährung des Einsichtsrechts vorliege – mit Ausnahme, wo ein formelles Gesetz eine Einschränkung der Auskunft vorsehe[89] – bei der Frage der Einschränkung in jedem Fall eine Abwägung zwischen dem Anspruch des Auskunftsberechtigten und den entgegengesetzten, berechtigten Interessen des Inhabers der Datensammlung vorzunehmen sei[90]. Einen weiteren Grund für eine Einschränkung des Auskunftsrechts könnten überwiegende öffentliche Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, darstellen[91]. Dabei sei bei der gerichtlichen Prüfung der für und gegen die Einsicht sprechenden Gründe den verantwortlichen Behörden ein gewisser Beurteilungsspielraum zuzugestehen[92]. Jedoch müsse der Grund der Einschränkung des Auskunftsrechts vom Inhaber der Datensammlung angegeben werden[93].

Das BFM konnte darlegen, dass es dem Beschwerdeführer bereits Einsicht in die meisten Aktenstücke gewährt hatte; auch hatte das BFM nach Ansicht des beurteilenden Gerichts die Begründungspflicht für seine Einschränkung der Einsicht nicht verletzt. Hinsichtlich Akten anderer Bundesbehörden durfte das BFM auf diese als Inhaberinnen einer Datensammlung verweisen und die Einsicht in jene Aktenstücke verweigern, die keine Personendaten enthielten[94].

In einem Fall vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission[95] stellten sich Fragen zur Kostenübernahme des Einsichtsberechtigten. Ein Beschwerdeführer machte geltend, dass ihm gestützt auf Art. 8 DSG das Recht auf Akteneinsicht kostenlos zu gewähren sei;

87 A-7368/2006; bestätigt durch das Bundesgericht in BGer 1C 225/2007.
88 Damals Bundesamt für Flüchtlinge (BFF).
89 Art. 9 Abs. 1 Bst. a DSG.
90 Art. 9 DSG.
91 Art. 9 Abs. 2 Bst. a DSG.
92 BVerwG A-7368/2006; BGE 125 II 225 E. 4a.
93 Art. 9 Abs. 4 DSG.
94 A-7368/2006.
95 Urteil Nr. 10/98 des Präsidenten der Eidgenössischen Datenschutzkommission vom 15. März 1999 (= VPB 64.72).

dagegen stellte sich die betroffene Behörde zunächst auf den Standpunkt, dass sich die Gebührenerhebung nach dem bereits laufenden Verfahren richte, sowie, dass die Gewährung der Akteneinsicht im vorliegenden Fall mit einem besonders grossen Aufwand verbunden gewesen sei. Die Rekurskommission hielt fest, dass wenn eine betroffene Person den datenschutzrechtlichen Anspruch auf Auskunftserteilung geltend mache, darüber - jedenfalls nach Abschluss des Verfahrens - nicht mehr nach dem anwendbaren Verfahrensrecht zu entscheiden sei, sondern nach dem Datenschutzgesetz[96]. Das Vorliegen einer besonders aufwändigen Herausgabe von Akten wurde ebenfalls abgelehnt. Mit Bezug auf die Kostenbeteiligung habe der Verordnungsgeber bewusst tiefe Vorgaben gemacht, die zu erheben sich nur durch einen tatsächlich ausserordentlichen Aufwand rechtfertigen lassen würden[97].

Kantonale Entscheide zum Einsichtsrecht

Die Rechtsprechung zum Einsichtsrecht soll schliesslich noch anhand einiger kantonaler Entscheide dargestellt werden. Die kantonalen Behörden beurteilen die vorgebrachten Fälle zum Datenschutzrecht nach den kantonalen Datenschutzgesetzen oder weiteren einschlägigen Bestimmungen. Wo Bundesrecht vollzogen wird, kann das DSG zwar subsidiär als kantonales Recht herangezogen werden. In den betrachteten Urteilen zu den Einsichts- und Durchsetzungsrechten wurde jedoch kein Bundesrecht vollzogen. Die kantonalen Gerichte nahmen jedoch immer wieder auf das Datenschutzgesetz des Bundes Bezug, um (unklare) kantonale Bestimmungen zum Datenschutz auszulegen[98].

In einem kantonalen Verfahren zum Einsichtsrecht war etwa streitig, ob nahe Verwandte eines Verstorbenen, die einen Haftungsprozess gegen die diesen behandelnden Ärzte anstrengten, vollumfängliche Einsicht in die Akten erhalten dürfen. Obwohl es sich um nahe Verwandte handelte, verneinte die zuständige kantonale Behörde das Bestehen eines schutzwürdigen Interesses für die Einsicht in die vollständige Krankengeschichte und schützte den Entscheid der Vorgängerinstanz. Diese hatte entschieden, die Krankengeschichte nicht den Beschwerdeführenden selber, sondern nur einer ärztlichen Vertrauensperson herauszugeben und ihr auferlegt, die Angehörigen nur soweit über den Inhalt der Akten zu orientieren, als es zur Abklärung und Geltendmachung von zivilrechtlichen Ansprüchen notwendig sei[99].

In einem weiteren Verfahren ging es um die Frage des Umfangs des Akteneinsichtsrechts einer Rechnungs- und Geschäftsprüfungskommission eines Gemeinderates, der diese Einsicht verweigert hatte. Die zuständige Behörde hielt fest, dass einer Rechnungs- und Geschäftsprüfungskommission sehr weitgehende Einsichts- und Herausgaberechte zustehen würden – d.h. das Recht auf Einsicht in alle personenbezogenen Akten und in die Originalprotokolle des Gemeinderates; diese könnten nur durch den Schutz von Daten der Intimsphäre sowie durch den Schutz der unmittelbaren Entscheidfindung (laufende Geschäfte) des Gemeinderates eingeschränkt wer-

96 VPB 64.72, E. 2.
97 VPB 64.72.
98 Z.B. KGVVE BL vom 22.10.2003 i.S. W.E.
99 Entscheid des Regierungsrates AG vom 20.11.2002 i.S. M. und S. sowie M.M. gegen Gesundheitsdepartement.

den. Der der Rechnungs- und Geschäftsprüfungskommission das Akteneinsichtsrecht verweigernde Entscheid des Gemeinderates wurde aufgehoben[100].

In einem weiteren Fall im Zusammenhang mit dem Volksschulrecht hielt die zuständige Behörde fest, dass Recht auf Akteneinsicht (inkl. das Anfertigen von Fotokopien) auch hinsichtlich einer bereits erledigten Sache weiter bestehe. Nach verschiedenen Sitzungen stand fest, dass das Kind der Beschwerdeführer, das auf therapeutische Hilfe angewiesen war, in normale Primarschule eingeschult werden konnte. Anlässlich einer weiteren Sitzung erstellte die Präsidentin der zuständigen Schulpflege einen Rapport, für welchen den Beschwerdeführern keine Einsicht gewährt wurde; diese aber verlangten die Einsicht, um über die bei der Schulbehörde befindliche vollständige Information verfügen zu können[101]. Im Ergebnis, d.h. mit Blick auf die Erkenntnis, dass das Akteneinsichtsrecht auch hinsichtlich einer bereits erledigten Sache weiter bestehe, ist dieser Entscheid zu begrüssen, jedoch mit Blick auch einige Erwägungen erstaunlich: So wurde etwa das Interesse der Behörden, nicht alle Informationen aus dem Schülerdossier herauszugeben, höher gewichtet als das Interesse der Eltern, vom ganzen Dossier Kenntnis zu haben.

Ein weiteres Verfahren, das die Beschwerde eines Gemeinderates gegen die Zulässigkeit der Herausgabe von Adresslisten des Stimmregisters an eine Privatperson zur beabsichtigten Gründung eines Ortsvereins zum Gegenstand hatte, wurde teilweise gutgeheissen. Eine Privatperson verlangte die Adressen zum Zweck der Lancierung einer Initiative auf Eigentumserwerb durch den neu zu gründenden Verein. Der Gemeinderat durfte als Voraussetzung für die Herausgabe der Adressen insbesondere verlangen, dass die Privatperson die tatsächliche Lancierung der Initiative glaubhaft zu machen hat[102].

9.1.3 Fazit

Das Auskunfts- bzw. Einsichtsrecht wird von den Betroffenen im Vergleich zu den Durchsetzungsrechten nach Art. 15 und 25 DSG wesentlich häufiger geltend gemacht. Damit wird die grundsätzliche Bedeutung des Auskunftsrechts im Datenschutz – stellt das Auskunftsrecht doch letztlich eine Grundvoraussetzung für die Überprüfung der Einhaltung der Datenschutzgesetzgebung und der Ausübung der Kontrollrechte dar (sie wird damit sichergestellt, dass die Betroffenen über die bearbeiteten Daten informiert sind) – durch seine praktische Bedeutung unterstrichen. Das Instrument des Auskunftsrecht wird von den Betroffenen als recht wichtiges Instrument zur Durchsetzung ihrer Rechte angesehen.

In materieller Hinsicht lässt eine Gesamtschau der zahlreichen Urteile zum Auskunftsrecht – bei aller Vorsicht, mit der solche Verallgemeinerungen zu geniessen sind – folgende Schlüsse zu:

- Die Erfolgsrate von das Auskunftsrecht betreffenden Klagen ist insbesondere vor höheren Gerichten relativ hoch, so dass sich der Schluss aufdrängt, dass die Einsichtsrechte – sofern sie überhaupt geltend gemacht werden – insgesamt recht wirksam geschützt werden.

---

100 KGVVE BL vom 22.10.2003 i.S. W.E.
101 Urteil des Verwaltungsgerichtshofes des Kantons Freiburg vom 17.12.2002.
102 Kanton Aargau; Entscheid des Regierungsrates vom 27.8.1984 i.S. Gemeinderat Wettingen gegen Departement des Innern.

- Damit einher geht die Feststellung, dass bei der häufig entscheidenden Abwägung dem Auskunftsrecht ein hohes Gewicht eingeräumt wird und – entsprechend der Anlage des Gesetzes – das Recht auf Auskunft als Regel angesehen wird, so dass die Ausnahmen eher restriktiv ausgelegt werden und sich der Eindruck aufdrängt, die (insbesondere die höheren) Gerichte entscheiden im Zweifel zugunsten des Auskunftsrechts.
- Bestätigt wird durch die Rechtsprechung, dass das Recht auf Auskunft auch und gerade das Recht umfasst, Kopien der vorhandenen Daten zugestellt zu bekommen.
- Weiter ergibt sich aus der Rechtsprechung, dass die Einstufung bestimmter Dokumente als „intern" die Tragweite des Auskunftsrechts nicht grundsätzlich modifizieren darf; in der Gerichtspraxis dürfen keine weiteren als die in den Art. 9 und 10 DSG aufgeführten Ausnahmen zur Beschränkung des Einsichtsrechts gebildet werden.
- Von nicht zu unterschätzender praktischer Bedeutung ist auch der durch die Rechtsprechung betonte Grundsatz, dass die Verfahren nach Art. 8 DSG auch dann geltend gemacht werden konnten, wenn sich das Hauptverfahren primär nach spezialgesetzlichen, z.B. sozialversicherungsrechtlichen, Bestimmungen richtete. Die Geltendmachung der datenschutzrechtlichen Grundsätze konnte einerseits im gleichen Verfahren erfolgen und für diesen Fall stellten die Gerichte sicher, dass – sofern die Einsichtsrechte nach Art. 8 des DSG weitere Rechte begründeten als die spezialgesetzlichen Vorschriften – die Bestimmungen zum Einsichtsrecht nach DSG vollständig gewährt wurden, d.h. nicht durch vorgehende spezialgesetzliche Regelungen beschränkt wurden. Andererseits wurde sichergestellt, dass Einsichtsrechte nach Art. 8 DSG auch in einem separaten Verfahren geltend gemacht werden konnten.

Unabhängig von der Frage, ob jedes einzelne Urteil zu diesem Fragenkomplex zu überzeugen vermag (deren Beantwortung den Rahmen der vorliegenden Untersuchung sprengte), drängt sich damit insgesamt die Schlussfolgerung auf, dass sich das Auskunftsrecht als Instrument der Betroffenen, ihre Rechte geltend zu machen, wohl insgesamt bewährt hat. Es ist nicht ersichtlich, dass der Geltendmachung des Auskunftsrechts insofern ins Gewicht fallende Hindernisse entgegenstehen, als die Betroffenen sich nicht auf dieses Recht (gerichtlich) berufen würden.

Allerdings besteht eine bereits angesprochene Schwierigkeit fort: Das Auskunftsrecht kann von den Betroffenen von Vornherein nur dann geltend gemacht werden, wenn sie über die Datenbearbeitung grundsätzlich informiert sind. Angesichts der Tatsache, dass eine grosse Zahl der Betroffenen vermutlich nicht über die tatsächliche Bearbeitung ihrer Daten Kenntnis hat, muss die beschriebene relativ häufige Inanspruchnahme jedoch ein Stück weit relativiert werden.

Soweit es um die Datenbearbeitung durch Bundesorgane geht, dürfte dieser Aspekt jedenfalls in Zukunft insofern weniger problematisch sein, als mit der am 1.12.2010 in Kraft getretenen Revision des DSG eine Erweiterung der Informationspflicht der Bundesorgane einhergeht, müssen diese doch nunmehr über jegliche Beschaffung von Personendaten grundsätzlich spontan und umfassend informieren (Art. 18a DSG). Für Private hingegen besteht eine ausdrückliche Informationspflicht der Beschaffung von Personendaten lediglich für Persönlichkeitsprofile und besonders sensible Personendaten (Art. 14 DSG); ansonsten kommt nur der Grundsatz der Erkennbarkeit (Art. 4 Abs. 4 DSG) zum Zuge. Ob dieser wirklich angesichts der vielfältigen Bear-

beitungen sowie Bearbeitungsmöglichkeiten Privater und ihrer entsprechenden Interessen als ausreichend angesehen werden kann, ist zumindest gewissen Zweifeln unterworfen.

9.2 Rechtsansprüche bei der Datenbearbeitung durch Privatpersonen

9.2.1 Inhalt des Durchsetzungsrechts (Art. 15 DSG)

Gemäss Art. 12 Abs. 1 DSG sind Private gehalten, bei der Datenbearbeitung die Persönlichkeit der betroffenen Personen nicht widerrechtlich zu verletzen.

Eine widerrechtliche Datenbearbeitung durch Private liegt insbesondere dann vor, wenn die betreffenden Personendaten entgegen den allgemeinen datenschutzrechtlichen Grundsätzen bearbeitet werden, wenn Private Daten ohne Rechtfertigungsgrund gegen den ausdrücklichen Willen der Betroffenen bearbeiten und wenn ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt gegeben werden[103].

Allgemein gesprochen stellt somit die Bearbeitung von Personendaten durch private Bearbeiter eine widerrechtliche Persönlichkeitsverletzung dar, wenn nicht ein Rechtfertigungsgrund vorliegt.

Die in Frage kommenden Rechtfertigungsgründe, welche die Widerrechtlichkeit der Persönlichkeitsverletzung aufzuheben vermögen, werden in Art. 13 Abs. 1 DSG aufgezählt. Die Verletzung der Persönlichkeit ist demnach nicht widerrechtlich, wenn sie durch die Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch eine gesetzliche Grundlage gerechtfertigt wird.

Die Bestimmungen (Art. 12, 13 DSG) lehnen sich damit stark an die Bestimmungen zum Persönlichkeitsschutz im Zivilgesetzbuch an. Art. 28 Abs. 1 ZGB hält fest, dass jede Person, die in ihrer Persönlichkeit widerrechtlich verletzt werde, zu ihrem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen könne. Nach Art. 28 Abs. 2 ZGB ist die Verletzung widerrechtlich, wenn sie nicht durch die Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist[104].

Mit Blick auf die Bestimmung des überwiegenden Interesses der bearbeitenden Person (überwiegendes privates Interesse) listet Art. 13 Abs. 2 DSG eine Anzahl Indizien auf, die auf das Vorliegen eines überwiegenden privaten Interesses hinweisen können – aber nicht müssen. Bestandteil dieser nicht abschliessenden Reihe von Indizien sind z.B. der unmittelbare Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags, die Prüfung der Kreditwürdigkeit einer Person, die Veröffentlichung in den Medien (redaktioneller Teil) oder die Bearbeitung von Daten über eine Person des öffentlichen Lebens[105].

---

[103] Art. 12 Abs. 2 DSG.

[104] In einem Reko-Urteil etwa wurde festgehalten, dass das DSG die Widerrechtlichkeit der Persönlichkeitsverletzung im Sinne des ZGB als Anknüpfungsgrund nehme und entsprechend für jede Form der Datenbearbeitung durch Private einen Rechtfertigungsgrund verlangt Urteil Nr. 12/01 (=VPB 68.68) der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 29. August 2003.

[105] Art. 13 Abs. 2 Bst. a, c, d und f DSG.

In Art. 12 Abs. 3 DSG wird festgehalten, dass in der Regel keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat[106].

Art. 15 regelt die Durchsetzungsrechte der durch eine private Datenbearbeitung betroffenen Personen, durch die ihre Persönlichkeit widerrechtlich verletzt wurde, wird oder eine entsprechende Verletzung droht, sowie das entsprechende Verfahren zur Durchsetzung dieser Ansprüche.

Art. 15 DSG nimmt Bezug auf das Verfahren zur Geltendmachung einer Persönlichkeitsverletzung mittels widerrechtlicher Datenbearbeitung durch Private und verweist für Klagen und vorsorgliche Massnahmen zum Schutz der Persönlichkeit auf Art. 28, 28a und 28l des Zivilgesetzbuches (ZGB)[107]. Wenn Bundesorgane privatrechtlich handeln, finden ebenfalls die Grundsätze von Art. 15 DSG Anwendung.

Art. 15 Abs. 3 DSG sieht eine Reihe von Rechten bzw. Ansprüchen für die durch die Datenbearbeitung betroffene Person vor, nämlich das Recht auf Berichtigung, auf Vernichtung und auf Sperrung ihrer persönlichen Daten. Darunter fällt insbesondere das Recht auf die Sperrung der Bekanntgabe ihrer persönlichen Daten an Dritte; ebenso kann verlangt werden, dass ein Bestreitungsvermerk[108] oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

9.2.2 Qualitative Analyse

Im Folgenden sollen die charakteristischen Fälle, welche hinsichtlich der Datenbearbeitung durch Private in der Gerichtspraxis von Bedeutung waren, kurz vorgestellt werden. Wie die quantitative Analyse der Rechtsprechung zeigen konnte, ist Art. 15 DSG kaum Gegenstand von Gerichtsurteilen. Soweit es um die Zulässigkeit einer Datenbearbeitung durch Private als solche geht, betreffen die zu analysierenden Fälle insbesondere die Rechtfertigungsgründe im Sinne von Art. 13 Abs. 1 DSG, d.h. die Einwilligung des Verletzten, die Interessenabwägung und Fragen zum Vorliegen einer gesetzlichen Grundlage, welche die Datenbearbeitung rechtfertigen könnte. Es soll untersucht werden, wie diese Rechtfertigungsgründe von den rechtsanwendenden Behörden ausgelegt werden.

Einwilligung des Verletzten

Vor dem Bundesverwaltungsgericht stellten sich Fragen zum Rechtfertigungsgrund der Einwilligung der betroffenen Person bei der Bearbeitung ihrer Daten durch Private. Zum Zweck der Missbrauchsbekämpfung bei der Benutzung persönlicher, nicht übertragbarer Eintrittsabonnemente in ein Hallenbad wurde ein Zugangskontrollsystem eingeführt, das für die unzweifelhafte Identifikation einer Person deren biometrische Daten speicherte. Gegen dieses Vorgehen erhob der EDÖB Beschwerde, und es stellte sich die Frage, ob sich die Hallenbadbetreiberin als Recht-

[106] Die Anforderungen sind dennoch rel. hoch, dass ein solches allgemeines Zugänglichmachen vorliegt; vgl. den Fall Spam-Mail der Eidgenössischen Datenschutz- und Rekurskommission.
[107] Art. 15 Abs. 1 DSG.
[108] Der Kläger hat insbesondere das Recht, bei Daten, deren Richtigkeit nicht nachgewiesen werden kann, einen Bestreitungsvermerk anbringen zu lassen; Art. 15 Abs. 2 DSG.

fertigungsgrund für ihre Datenbearbeitung auf die Einwilligung der Käufer der Abonnemente stützten konnte[109].

Das Bundesverwaltungsgericht führte zum Erfordernis der Einwilligung nach Art. 4 Abs. 5 DSG aus, dass diese eine angemessene Information bezüglich der Datenbearbeitung voraussetze, in die eingewilligt werden soll. Des Weiteren müsse eine Willenserklärung des Betroffenen vorliegen, aus der die Zustimmung zu dieser Datenbearbeitung abgeleitet werden könne. Die Einwilligung müsse insbesondere *freiwillig* erfolgen, das heisst Ausdruck des freien Willens der betroffenen Person sein. Ungültig sei demnach die durch Täuschung, Drohung oder Zwang zustande gekommene Einwilligung. Der betroffenen Person müsse „eine – mit nicht unzumutbaren Nachteilen behaftete – Handlungsalternative" zur Verfügung stehen[110].

Im vorliegenden Fall wurde von der Badbetreiberin nur dann ein herkömmliches Badeabonnement erteilt, wenn sich ein Gast geweigert hatte, ein biometrisches Abonnement zu lösen. Durch diese Vorgehensweise sah das Bundesverwaltungsgericht den Grundsatz der Freiwilligkeit der Einwilligung und auch die Informationspflicht hinsichtlich der Einwilligung durch die Hallenbadbetreiberin verletzt. Die Betreiberin könne sich demnach nicht auf eine Einwilligung der Käufer berufen, die ihre Datenbearbeitung im Sinne von Art. 13 Abs. 1 DSG hätte rechtfertigen können[111].

In einem weiteren Fall hatte sich die Rekurs- und Öffentlichkeitskommission mit der Frage der Zulässigkeit von Drogentests auseinanderzusetzen. Für den Eintritt in ein Unternehmen mussten Lehrstellen-Bewerberinnen und -Bewerber einen Fragebogen bezüglich ihres Gesundheitszustandes ausfüllen. Die Aufnahme in die Lehrstelle erfolgte unter dem Vorbehalt einer ärztlichen Untersuchung und eines Drogenscreenings. Wer positiv auf harte Drogen getestet wurde, konnte zu diesem Zeitpunkt nicht in die Lehre aufgenommen werden. Sowohl bei Lehrbeginn als auch anschliessend stichprobenweise (zweimal pro Jahr) während der Lehre wurden weitere Drogentests durchgeführt. Als der EDÖB eine Stellungnahme des Unternehmens zu seinem Vorgehen verlangte, stütze sich dieses auf die schriftliche Einwilligung der Auszubildenden und deren Eltern[112].

Auch hier stellte sich für das Bundesverwaltungsgericht die Frage, ob die auszubildenden Personen tatsächlich freiwillig eingewilligt hatten. Damit eine Einwilligung zur Datenerhebung als Rechtfertigungsgrund gemäss Art. 13 Abs. 1DSG in Betracht gezogen werden könne – so das Gericht –, müsse insbesondere gewährleistet sein, dass diese Einwilligung mit Art. 27 Abs. 2 ZGB im Einklang stehe. Hierzu sei erforderlich, dass sie freiwillig und in Kenntnis ihrer rechtlichen Tragweite erfolgt. Bei der Beurteilung sei auf die tatsächliche Situation im Einzelfall abzustellen.

In seiner Stellungnahme zeigte das betroffene Unternehmen auf, dass alle Interessentinnen und Interessenten, die sich für eine Lehrstelle bewarben, vorgängig ausführlich über das Konzept der

---

109 BVGE 2009/44, Urteil vom 4. August 2009.
110 BVGE 2009/44, Erw. 4.2; Urteil vom 4. August 2009.
111 BVGE 2009/44, Urteil vom 4. August 2009. Im Urteil wurde zudem das Vorliegen von überwiegenden privaten Interessen geprüft; Erw. 5.
112 Urteil 12/01 der Eidgenössischen Datenschutzkommission vom 29. August 2003 (=VPB 68.68).

drogenfreien Lehre informiert wurden. Zudem wurde angeführt, dass keine Person gezwungen worden sei, sich um eine Lehrstelle beim betreffenden Unternehmen zu bewerben und diese anschliessend anzutreten.

Nach der Ansicht des Bundesverwaltungsgerichts griff diese Argumentation zu kurz. Denn gerade wenn es für junge Leute schwierig sei, einen Ausbildungsplatz zu finden, seien sie eher bereit, Konzessionen einzugehen, wenn es darum gehe, eine geeignete oder sogar die «Wunsch»-Lehrstelle zu finden. Wenn man allenfalls noch von Freiwilligkeit sprechen könnte, sich vor Antritt der Lehrstelle einem Screening zu unterziehen, dann gelte dies jedoch sicher nicht mehr in Bezug auf die Screenings, die während der Lehrzeit durchgeführt würden.

Die Auszubildenden seien sich wohl bewusst, dass ein Ablehnen eines solchen Tests als Verstoss gegen die vertraglich getroffene Vereinbarung angesehen und wohl auch entsprechende Konsequenzen nach sich zöge. Die jeweils abzugebende Einwilligung sei somit nicht als freiwillig zu betrachten und genüge deshalb nicht als Rechtfertigungsgrund für die Durchführung der Tests und die damit verbundenen Datenerhebungen; sie sei eine Verletzung der Persönlichkeit[113].

Vor dem Bundesgericht stellten sich Fragen zum Rechtfertigungsgrund der Einwilligung, so z.B. bei der Geltendmachung der Herausgabe von Patientenakten bei einer Praxisübernahme, und zwar danach, ob und wie die Weitergabe der Patientendossiers gestützt auf die gültige Einwilligung der Patienten zu rechtfertigen sei[114]. Das Gericht hielt fest, dass die Personendaten der Patientenkartei einer Arztpraxis grundsätzlich dem durch Art. 28 ZGB geschützten Geheimbereich der betreffenden Patientinnen und Patienten zuzurechnen seien. Die Weitergabe solcher Daten bedeute eine Persönlichkeitsverletzung, die nach Art. 28 Abs. 2 ZGB nur dann nicht widerrechtlich sei, wenn sie durch Einwilligung der Betroffenen, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt sei. Daten, die über die Gesundheit von Personen Auskunft geben, gehörten zudem zu den besonders schützenswerten Personendaten[115], deren Weitergabe an Dritte auch nach Art. 12 Abs. 2 Bst. c DSG i.V.m. Art. 3 Bst. f DSG eine Persönlichkeitsverletzung indiziere[116].

Das Bundesgericht führte weiter aus, dass dem Erfordernis der Einwilligung bei einer Praxisübergabe grundsätzlich ohne Weiteres entsprochen werden könne, wenn der die Praxis veräussernde Arzt sich genügend Zeit nehme, um seinen Patientinnen und Patienten die beabsichtigte Praxisübergabe anzuzeigen und ihre Einwilligung zur Weitergabe der Krankengeschichten an einen Nachfolger einzuholen. Würde sich der Veräusserer einer Praxis vorbehaltlos zur Übertragung der gesamten Patientenakten verpflichten, so übernehme er damit auch die Verpflichtung, alles zu unternehmen, um die Zustimmung der Patienten zur Übertragung ihrer Akten auf den Übernehmer der Praxis einzuholen[117].

---

113 Urteil 12/01 der Eidgenössischen Datenschutzkommission vom 29. August 2003 (=VPB 68.68).
114 BGE 135 III 433.
115 Art. 3 Bst. a Ziff. 2 DSG.
116 BGE 135 III 433.
117 BGE 135 III 433.

Die Analyse der Rechtsprechung zur Einwilligung des Betroffenen zeigt somit insgesamt, dass an das Vorliegen dieses Rechtfertigungsgrundes, insbesondere mit Blick auf die Freiwilligkeit, in der Gerichtspraxis (zu Recht) hohe Anforderungen gestellt werden.

Rechtfertigung durch Gesetz

Ein Fall, bei dem das Bundesverwaltungsgericht die Datenbearbeitung als durch Gesetz gerechtfertigt angesehen hatte, ergab sich mit Bezug auf das Schweizerische Handelsamtsblatt (SHAB). Ein Unternehmen bezog vom SHAB Handelsregisterdaten. Diese Daten wurden insbesondere durch ein Personensuchparameter ergänzt und im Internet publiziert, sodass sämtliche einmal im SHAB veröffentlichten Daten zu natürlichen und juristischen Personen zeitlich unbeschränkt und kostenlos eingesehen werden konnten[118]. Der EDÖB erliess eine Empfehlung an das die Daten publizierende Unternehmen und erhob nach deren Ablehnung Beschwerde beim Bundesverwaltungsgericht mit dem Antrag, die nicht mehr aktuellen Handelsregistereinträge nach Ablauf von drei Jahren oder auf Begehren seien zu löschen[119].

Für das Bundesverwaltungsgericht stellte sich die Frage, ob die Datenbearbeitung durch das betreffende Unternehmen durch das Vorliegen einer gesetzlichen Grundlage gerechtfertigt werden konnte. Nach der gesetzlichen Vermutung von Art. 12 Abs. 3 DSG liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat, ohne die Bearbeitung ausdrücklich zu verbieten. Für die Angaben, die natürliche Personen für Handelsregistereinträge gegenüber der Handelsregisterbehörde zu machen haben, besteht jedoch eine gesetzliche Eintragungspflicht. Art. 12 Abs. 3 DSG sei, so das Bundesverwaltungsgericht, nicht anwendbar, wenn – wie im vorliegenden Fall – das betreffende Unternehmen gesetzlich dazu verpflichtet sei, seine SHAB-relevanten Daten zu publizieren. Der Ausschlussgrund für eine mögliche Persönlichkeitsverletzung komme damit im vorliegenden Fall nicht zum Tragen[120].

Gemäss Art. 12 Abs. 2 Bst. b DSG liegt eine Persönlichkeitsverletzung insbesondere dann vor, wenn eine Datenbearbeitung gegen den ausdrücklichen Willen der betroffenen Personen erfolgt und kein Rechtfertigungsgrund dafür vorliegt. Das Bundesverwaltungsgericht prüfte daher weiter, ob sich die Beklagte für ihre Weigerung, Löschbegehren stattzugeben, auf einen Rechtfertigungsgrund gemäss Art. 13 Abs. 1 DSG stützen konnte.

Nicht widerrechtlich – so das Bundesverwaltungsgericht – sei eine Datenbearbeitung dann, wenn das Gesetz die Bearbeitung von Personendaten ausdrücklich vorschreibe, erlaube oder implizit voraussetze[121]. Die private Weiterverbreitung der – öffentlichen und ohne besonderes Interesse zugänglichen – Handelsregisterdaten diene dem Zweck der informationellen Erleichterung des Geschäftsverkehrs, solange die Daten unverändert von einem staatlichen Referenzdatenbestand

[118] Im SHAB sind die entsprechenden Daten nur beschränkt, insbesondere nur während dreier Jahre zugänglich. Eine personenbezogene Suche ist nicht oder nur sehr eingeschränkt möglich.
[119] BVGE 2008/16, Urteil vom 26. Februar 2008.
[120] BVGE 2008/16, Urteil vom 26. Februar 2008.
[121] Mit dem Begriff „durch Gesetz“ werde dabei demgegenüber kein Gesetz im formellen Sinne als rechtfertigende Grundlage verlangt.

übernommen und weiterverbreitet werden[122]. Das Bundesverwaltungsgericht erinnerte insbesondere an die Pflicht für private Bearbeiter von Handelsregisterdaten aus dem SHAB, die übernommenen Daten inhaltlich nicht zu verändern[123]. Die längere Datenspeicherung sei daher zulässig; Datenlöschungen führten hingegen dazu, dass gewisse nach wie vor geltende Handelsregisterinformationen als nicht mehr existent erachtet werden könnten; die entstehende Intransparenz unterliefe den Zweck der informationellen Erleichterung des Geschäftsverkehrs. Die Datenbearbeitung durch die Beklagte sei demnach durch Gesetz im Sinne von Art. 13 Abs. 1 DSG gerechtfertigt. Der Fall ist insofern typisch, als er die Tendenz in der Rechtsprechung darstellt, beim Vorliegen einer gesetzlichen Grundlage die Bearbeitungen relativ grosszügig zuzulassen; der Rechtfertigungsgrund wird generell weniger eingehend geprüft als der Rechtfertigungsgrund der Einwilligung des Betroffenen (dazu vertieft noch unten).

Rechtfertigung durch überwiegende private oder öffentliche Interessen

Die Gerichte hatten sich mit Bezug auf die vom Gesetz vorgesehenen Rechtfertigungsgründe der Einwilligung des Verletzten, der gesetzlichen Grundlage und der überwiegenden öffentlichen oder privaten Interessen[124] in einer deutlichen Mehrzahl der Fälle mit dem zuletzt genannten und nun aus der Gerichtspraxis darzustellenden Rechtfertigungsgrund auseinander zu setzen, d.h. mit der Abwägung der einander gegenüberstehenden Interessen. Dabei spielte die Abwägung der Interessen der durch die Datenbearbeitung betroffenen Person gegenüber möglicherweise überwiegenden öffentlichen Interessen eine untergeordnete Rolle. Im Vordergrund stand die Abwägung gegenüber den privaten Interessen des Bearbeitenden.

Die Fälle zu den öffentlichen Interessen betrafen etwa medienrechtliche Fragen sowie Fragen zur Datenbearbeitung über Personen des öffentlichen Lebens. In einem Fall, den das Bundesgericht zu beurteilen hatte, wurde einer relativ bekannten Person durch einen Redaktor mitgeteilt, dass über sie in einer Wochenzeitschrift demnächst ein Portrait erscheinen werde. Der Betroffene untersagte explizit die Veröffentlichung des Berichts. Dessen ungeachtet erschien der Artikel mit seinem Bild. Der Betroffene sah darin eine Persönlichkeitsverletzung im Sinne von Art. 28a Abs. 1 Ziff. 3 ZGB.

Ein überwiegendes öffentliches Interesse wird gemäss Art. 13 Abs. 2 Bst. d DSG vermutet, wenn die Bearbeitung der Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums erfolgt. In der Rechtsprechung der Gerichte wird betont, dass die Veröffentlichung im redaktionellen Teil eines Mediums dennoch keinen absoluten Rechtfertigungsgrund darstelle; damit solle dem Gericht vielmehr ein Beurteilungselement für die

[122] Dies ergibt sich aus der Konzeption der Öffentlichkeit des Handelsregisters gemäss Art. 930 OR und aus den verschiedenen gesetzlichen Bestimmungen zur Funktionsweise und zur Publikation der Handelsregisterdaten, wie die folgenden Bestimmungen: Art. 12 Abs. 1 HRegV, wonach die Kantone ihre Handelsregister ebenfalls über Internet unentgeltlich zugänglich machen müssen; Art. 35 Abs. 3 HRegV, wonach die Kantone die Handelsregisterinformationen nach der Publikation im SHAB auch in anderen Publikationsorganen veröffentlichen dürfen; Art. 12 und Art. 13 Verordnung SHAB, worin die Weitergabe an private Datenanbieter zwecks Verwertung explizit vorgesehen ist.

[123] Art. 13 Abs. 1 Bst. b Verordnung SHAB.

[124] Art. 13 Abs. 1 DSG.

vorzunehmende Interessenabwägung in die Hand gegeben werden[125]. Letztlich gehe es darum, die sorgfältige Abwägung des Interesses des Einzelnen auf Unversehrtheit seiner Person gegen das Interesse der Presse auf Information der Allgemeinheit vorzunehmen, um so die Anliegen von Persönlichkeitsschutz und Informationstätigkeit der Medien so weit als möglich miteinander in Einklang zu bringen. Dabei sei derselbe Massstab anzulegen wie bei der Beantwortung der Frage, ob sich die Berichterstattung über den Kläger an sich mit einem überwiegenden öffentlichen Informationsinteresse rechtfertigen lasse.

Vorliegend hatte das Bundesgericht die Persönlichkeitsverletzung mittels Berichterstattung als durch ein überwiegendes öffentliches Interesse gerechtfertigt beurteilt[126]. Bei Personen, die relativ bekannt sind, sei das Interesse der Öffentlichkeit, über sie in den Medien erfahren zu dürfen, relativ hoch zu gewichten. Insbesondere bei einer Berichterstattung der Medien über eine Person des öffentlichen Interesses komme dem öffentlichen Interesse bei fehlender Einwilligung des Verletzten ein grosses Gewicht zu[127].

Zur Abwägung der Interessen der durch die Datenbearbeitung betroffenen Person und den diesen gegenüberstehenden privaten Interessen ergaben sich in der Rechtsprechung verschiedene Fallgruppen, insbesondere zum Bereich Arbeitsverhältnis.

Die Frage, ob ein überwiegendes privates Interesse die Widerrechtlichkeit einer Persönlichkeitsverletzung durch die Datenbearbeitung zu beseitigen vermag, stellte sich vor dem Bundesgericht z.B. im folgenden Fall[128]: Eine Verkäuferin hatte sich gegen ihren Arbeitgeber zur Wehr gesetzt, weil dieser ihr während 5 Jahren einen tieferen als den im Gesamtarbeitsvertrag vorgesehenen Mindestlohn bezahlte. Für die Festsetzung des anzupassenden Lohns hatte sich der Arbeitgeber über die Gewerkschaftszugehörigkeit der Klägerin erkundigt.

Art. 13 Abs. 2 Bst. a DSG hält fest, dass eine Verletzung des Persönlichkeitsrechts insbesondere dann durch ein überwiegendes privates Interesse gerechtfertigt sein kann, wenn die Bearbeitung von Personendaten in direktem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und die bearbeiteten Daten den Vertragspartner betreffen. Im Fall des Arbeitsvertrages präzisiert der mit dem DSG in Kraft getretene Art. 328b OR, dass der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten (bzw. beschaffen) darf, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.

Obschon zweifelhaft sei, ob der Arbeitgeber sich vor der Anstellung über die Zugehörigkeit eines Arbeitnehmers zu einer Gewerkschaft erkundigen dürfe, erscheine – so das Bundesgericht – eine solche Frage hingegen zulässig, wenn sie nach Abschluss des Arbeitsvertrages gestellt werde und den Zweck habe, festzustellen, ob der Lohn des neuen Mitarbeiters den Vorschriften des bindenden Gesamtarbeitsvertrages entsprechen müsse. Eine diesbezügliche Auskunft stehe daher im Einklang mir den Bestimmungen von Art. 328b OR[129].

[125] BGE 127 III 481.
[126] BGE 127 III 481.
[127] BGE 127 III 481.
[128] BGE 123 III 129.
[129] BGE 123 III 129.

Auch in einem weiteren Fall hatte sich das Bundesgericht mit der Frage auseinanderzusetzen, ob der Persönlichkeitsschutz des Bewerbers dem Interesse des Arbeitgebers vorgehen sollte[130]. Die Beschwerdeführerin hatte sich für eine Telefonistenstelle bei einer Telefonmarketingfirma beworben, sich jedoch geweigert, einen ihre geschützte Persönlichkeitssphäre teilweise missachtenden Fragekatalog auszufüllen. Der Katalog enthielt nicht nur Fragen zu arbeitsplatzspezifischen Sachverhalten, sondern es ging um persönlichkeitskennzeichnende Merkmale wie Freizeitverhalten und sonstiges Privatleben, die im Hinblick auf die fragliche Stelle ohne Belang waren und damit klarerweise die schützenswerte Privatsphäre betrafen. Das Bundesgericht führte aus, dass die Telefonistin bei der betroffenen Firma keine besondere Vertrauensstellung bekleidete. Demnach könne der Arbeitgeber kein überwiegendes Interesse an Auskünften, die den Privatbereich der Beschwerdeführerin betreffen, geltend machen[131].

Die Frage des überwiegenden privaten Interesses als Rechtfertigungsgrund zur Datenbearbeitung von Angestellten stellte sich auch in einem weiteren, strafrechtlichen Verfahren vor dem Bundesgericht[132]. Ein Uhren- und Juweliergeschäft erstattete gegen eine seiner Angestellten Strafanzeige wegen Diebstahls; angeblich hatte die Angestellte aus der Kasse des Geschäfts Geld entwendet. Das Unternehmen stützte seine Aussagen auf Bilder einer Videokamera, die es ohne das Wissen der Mitarbeitenden im Geschäftsraum installiert hatte. Auf diesem Film sei ersichtlich, wie die betreffende Angestellte mit einem Tablett in der Hand den Kassenraum betrete, der Kasse Banknoten entnehme, diese auf das Tablett lege, mit einem Blatt Papier bedecke und mit dem Tablett in der Hand den Kassenraum verlasse. Die betreffende Angestellte bestritt, Geld entwendet zu haben. In der Beschwerde in Strafsachen war insbesondere die Rechtmässigkeit und die Verwertbarkeit der Filmaufnahmen als Beweismittel strittig[133].

Das Bundesgericht führte aus, dass die Überwachung der Arbeitnehmer am Arbeitsplatz durch Videokameras grundsätzlich geeignet sei, die Persönlichkeit der Arbeitnehmer zu verletzen und gegen Vorschriften des Datenschutzgesetzes zu verstossen[134]. Es stellte sich dabei wiederum die Frage, ob sich das Unternehmen, welches die Angestellte angezeigt hatte, auf den Rechtfertigungsgrund des überwiegenden persönlichen Interesses berufen konnte[135].

In diesem Zusammenhang wies das Bundesgericht darauf hin, dass sich im Kassenraum eines Uhren- und Juweliergeschäfts Bargeldbeträge in beträchtlicher Höhe befinden können. Daher habe der Geschäftsinhaber ein erhebliches Interesse an der Überwachung des Kassenraums. Die Videoüberwachung des Kassenraums sei zudem nicht ausschliesslich für die Überwachung des Personals erfolgt, sondern insbesondere für die Verhinderung von Straftaten durch Dritte. Des Weiteren führte das Bundesgericht aus, dass die Arbeitnehmer des Geschäfts von der Videoüberwachung im Kassenraum im Verlauf eines Arbeitstages nur sporadisch und kurzzeitig erfasst würden und verneinte daher unter den gegebenen Umständen eine widerrechtliche Persönlich-

130 BGE 122 V 267.
131 BGE 122 V 267.
132 BGr. 6B 536/2009, Urteil vom 12. November 2009.
133 BGr 6B 536/2009, Urteil vom 12. November 2009.
134 Art. 12 f. DSG, Art. 28 ZGB, Art. 328 und Art. 328b OR.
135 Art. 13 Abs. 1 DSG.

keitsverletzung im Sinne von Art. 28 ZGB, Art. Art. 12 Abs. 1 DSG[136]. Die konkrete Videoaufnahme sei daher für das betreffende Verfahren kein unrechtmässig erlangtes Beweismittel[137].

9.2.3 Fazit

Bei der überwiegenden Mehrzahl der hier kurz dargestellten, typischen Fallkonstellationen und aller übriger betrachteter Fälle waren die Beschwerdeführer bei der Geltendmachung der Verletzung von Persönlichkeitsrechten aufgrund der widerrechtlichen Datenbearbeitung seitens Privater nicht erfolgreich.

In einer Mehrzahl der Fälle war die Bearbeitung der persönlichen Daten durch überwiegende öffentliche oder private Interessen oder durch Gesetz gerechtfertigt[138].

An die Einwilligung und insbesondere die Freiwilligkeit der Einwilligung wurden von den Gerichten hingegen – mit Bezugnahme auf die Praxis und Literatur zu Art. 28 Abs. 2 ZGB – strenge Anforderungen gestellt, sodass nur wenige der vorgebrachten Datenbearbeitungen gestützt auf die Einwilligung der durch Datenbearbeitung betroffenen Personen gerechtfertigt werden konnten.

Aus prozessrechtlicher Sicht ergeben sich keine Hinweise auf spezielle, spezifische Schwierigkeiten zur Anrufung des Durchsetzungsrechts. Anzumerken ist jedoch, dass als Anspruchsgrundlage für das Durchsetzungsrecht nicht Art. 15 DSG, sondern andere Bestimmungen, insbesondere Art. 28 ff. ZGB, herangezogen werden[139].

Durch den Verweis auf Art. 28 ff. ZGB werden insbesondere mit Bezug auf die Freiwilligkeit der Einwilligung klare, durch Lehre und Rechtsprechung genau definierte Massstäbe herangezogen, anhand derer die Widerrechtlichkeit der Datenbearbeitung durch die Privatperson in materiellrechtlicher Hinsicht beurteilt werden kann[140].

9.3 Rechtsansprüche und Verfahren nach Art. 15 DSG und nach Art. 28 ZGB

Art. 15 DSG nimmt explizit Bezug auf Art. 28 ff. ZGB, welche die Rechtsansprüche im Zivilprozess regeln. Nachfolgend wird das Zusammenspiel der beiden Bestimmungen in der Rechtsprechung näher untersucht.

9.3.1 Charakteristische Fälle und Zusammenspiel der Bestimmungen

Bei Persönlichkeitsverletzungen aufgrund von widerrechtlichen Datenbearbeitungen durch Private stehen Art. 15 DSG und Art. 28 ff. ZGB in einer engen Beziehung.

---

136 Dies gelte auch für den Fall, dass die Beschwerdegegnerin nicht wusste, bzw. auch nicht mit der Möglichkeit rechnete, dass im Kassenraum eine Videokamera installiert und während der Geschäftszeit in Betrieb sein könnte.
137 BGr. 6B 536/2009, Urteil vom 12. November 2009.
138 Art. 13 DSG.
139 Dazu sogleich unten.
140 Vgl. hierzu insbesondere die Fälle zur Frage der rechtfertigenden Einwilligung durch den Betroffenen; oben.

Bei der Geltendmachung der Persönlichkeitsverletzung wird von den Gerichten in erster Linie auf Art. 28 Abs. 1 ZGB Bezug genommen, wonach jede Person, die in ihrer Persönlichkeit widerrechtlich verletzt wird, zu ihrem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen kann. Nach Art. 28 Abs. 2 ZGB ist die Verletzung widerrechtlich, wenn sie nicht durch die Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

Nach dem Wortlaut des DSG versteht sich Art. 15 als verfahrensrechtliche Verweisnorm zu Art. 28 ff. des ZGB[141]. So wurde auch in der Rechtsprechung auf den zivilrechtlichen Weg verwiesen, und zwar auf die Regeln des Persönlichkeitsschutzes im Sinne von Art. 28 ff. ZGB, beispielsweise um dem Massenversand unverlangter Werbe-E-Mails Einhalt zu gebieten[142]. Für die Geltendmachung der zu Art. 15 DSG erwähnten Fällen beriefen sich die Beschwerdeführer demnach nicht auf Art. 15 DSG im Sinne einer Anspruchsgrundlage; Anspruchsgrundlagen fanden sich in andern Erlassen, insbesondere in Art. 28 ZGB[143].

Für die Prüfung der Persönlichkeitsverletzung wird von den Gerichten demnach primär auf Art. 28 ZGB als Anspruchsgrundlage Bezug genommen, wo auch festgehalten wird, dass jede Verletzung der Persönlichkeit widerrechtlich ist. Art. 12 DSG nimmt die Widerrechtlichkeit auf und konkretisiert sie für den Bereich des Datenschutzes. In einem Urteil der Eidgenössischen Datenschutz- und Öffentlichkeitskommission wurde etwa festgehalten, dass sich das DSG die Widerrechtlichkeit jeder Persönlichkeitsverletzung im Sinne des Art. 28 ZGB zum Anknüpfungsgrund nimmt und entsprechend für jede Form der Datenbearbeitung durch Private einen Rechtfertigungsgrund verlangt[144].

In materiell-rechtlicher Hinsicht zeigt die Gerichtspraxis, dass sich die Bestimmungen ergänzen: Bei den Fällen, wo sowohl die Bestimmungen über die Datenbearbeitung durch Private nach dem DSG als auch Art. 28 ff. ZGB geltend gemacht wurden, geschah dies in einander ergänzender Weise. Das Bundesgericht führte entsprechend aus, dass die Regeln des DSG das Recht der Persönlichkeit des ZGB ergänzten und konkretisierten.

Besonders bei datenschutzrechtlichen Fragen im Zusammenhang mit dem Arbeitsverhältnis wurden die Bearbeitungsgrundsätze für Private des DSG, Art. 28 ff. ZGB und auch Art. 328 OR einander ergänzend herangezogen[145]. Ergänzend zur Anspruchsgrundlage werden demnach datenschutzrechtliche oder den Arbeitnehmer schützende Bestimmungen geprüft[146].

Gerade dort, wo Art. 15 DSG eigenständige Rechte vorsieht, namentlich beim Recht auf Anbringung eines Bestreitungsvermerks[147], wird diese Bestimmung explizit zusätzlich herangezogen. Die

---

141 „Für Klagen und vorsorgliche Massnahmen zum Schutz der Persönlichkeit gelten die Artikel 28 bis 28l des Zivilgesetzbuches"; Art. 15 Abs. 1 DSG. Der Artikel wurde mit Inkrafttreten auf den 1.1.2011 revidiert; der erste Satz der Bestimmung lautet nun: „Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28a sowie 28l des Zivilgesetzbuchs".

142 Z.B. Urteil Nr. 05/03 der Eidgenössischen Datenschutzkommission vom 15. April 2005 (= VPB 69.106).

143 Anstatt vieler BGE 135 III 433.

144 Urteil Nr. 12/01 (=VPB 68.68) der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 29. August 2003. Ausführungen zum Verhältnis der Durchsetzungsrechte finden sich in dieser Entscheidung nicht.

145 Vgl. z.B. das oben angeführte BGr 6B 536/2009, Urteil vom 12. November 2009.

146 Z.B. das vorher vorgestellte BGr 6B 536/2009, Urteil vom 12. November 2009.

147 Art. 15 Abs. 2 DSG.

datenschutzrechtlichen Bestimmungen werden auch zusätzlich herangezogen, um die Persönlichkeitsverletzung gestützt auf Art. 28 ZGB anhand der datenschutzrechtlichen Grundsätze zu beurteilen[148]. In einem Fall beispielsweise, bei dem es um die Frage der Zulässigkeit der Produktion und des Vertriebs eines Verzeichnisses der schweizerischen Fahrzeughalter auf CD-ROM durch eine Privatperson ging, wurde festgehalten, dass das DSG den Schutz des Einzelnen vor potentiellen Verletzungen seiner Persönlichkeit bezwecke und deshalb weiter gehe als der zivilrechtliche Persönlichkeitsschutz nach Art. 28 ZGB[149].

Die Geltendmachung von Rechten gestützt auf das DSG, etwa ein Verfahren über Einsichtsansprüche, das die Rechte Dritter tangieren kann, steht dem Anstrengen eines Verfahrens nach Art. 28 ff. ZGB nicht entgegen. So wurde in einer Entscheidung betreffend die Veröffentlichung von Akten festgehalten, es sei gesetzlich nicht vorgesehen, dass der Inhaber einer Datensammlung die Auskunft oder Einsicht einem Beschwerdeführer nur unter der Auflage erteilt, dass die Personen die betreffenden Daten nicht an Dritte weitergeben dürfen[150]. Würden durch die Weitergabe der betreffenden Information die Persönlichkeitsrechte Dritter tangiert, so stünden diesen selbst die Persönlichkeitsschutzmittel nach Art. 28 c Abs. 3[151] und Art. 28 g ff. (Recht auf Gegendarstellung) ZGB offen; diese letztgenannten Bestimmungen – so die Rekurskommission – würden dem DSG „vorgehen“[152]. „Vorgehen“ ist in diesem Fall u.E. in dem Sinne zu verstehen, dass diese Rechte von weiteren Betroffenen unabhängig von dem laufenden datenschutzrechtlichen Verfahren jederzeit herangezogen werden können.

Weiter ist darauf hinzuweisen, dass die weit entwickelte Praxis und Lehre zum Persönlichkeitsschutz nach Art. 28 ff. ZGB bei Persönlichkeitsverletzungen durch Datenbearbeitung durch Private nicht nur als Verweisnorm, sondern auch in materiell-rechtlicher Hinsicht zum Tragen kommt. So wurde in einem Urteil festgehalten, dass die Rechtfertigungsgründe nach Art. 13 Abs. 1 DSG denjenigen von Art. 28 Abs. 2 ZGB entsprechen. Entsprechend würden die von Lehre und ständiger Praxis zu Art. 28 Abs. 2 ZGB entwickelten Grundsätze auch im Bereich des DSG gelten. Insbesondere dürfe die Einwilligung des Betroffenen, um rechtswirksam zu sein, nicht ihrerseits gegen Art. 27 ZGB verstossen[153].

In einem Fall hatte sich das Bundesgericht mit der Frage der vorsorglichen Massnahmen im Sinne von Art. 15 DSG i.V.m. Art. 28c ZGB zu befassen[154]. Anlässlich seiner Entlassung verlangte ein Chefarzt von seinem arbeitgebenden Spital gestützt auf einen Antrag auf vorsorgliche Massnahmen die Herausgabe seines Personaldossiers und sämtlicher Daten, über die das Spital über

---

148 In einigen Entscheiden wurden die spezifischen datenschutzrechtlichen Probleme aber ausschliesslich auf Art. 28 ff. ZGB gestützt.

149 Entscheid Nr. 1/97 der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 18. März 1998.

150 Die Verfügungsbefugnis der betroffenen Person über ihr bekannte Informationen ergebe sich – so hielt das Gericht fest – aus dem Grundrecht auf informationelle Selbstbestimmung und aus der Meinungsäusserungsfreiheit.

151 Art. 28c Abs. 3 ZGB: Eine Verletzung durch periodisch erscheinende Medien kann das Gericht jedoch nur dann vorsorglich verbieten oder beseitigen, wenn sie einen besonders schweren Nachteil verursachen kann, offensichtlich kein Rechtfertigungsgrund vorliegt und die Massnahme nicht unverhältnismässig erscheint.

152 Urteil Nr. 9 und 10/96 der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 12. Oktober 1998; Beschwerde gegen diesen Entscheid vom Bundesgericht teilweise gutgeheissen; BGE 125 II 225.

153 Urteil Nr. 1/95_2 der Eidgenössischen Datenschutzkommission vom 21. November 1996 (= VPB 62.42B).

154 BGr. 4P.293/2006, Urteil vom 9.2.2007. Art. 15 Abs. 1 DSG wurde unterdessen revidiert; die vorsorglichen Massnahmen werden nicht mehr erwähnt; vgl. oben, Fn. 141.

ihn verfügte. Dem Antrag auf vorsorgliche Massnahmen wurde stattgegeben; das Spital setzte sich dagegen jedoch zur Wehr mit einer (unzulässigen) Berufung ans Bundesgericht.

Obwohl die Berufung unzulässig war, erfolgten in materieller Hinsicht einige Ausführungen. Das Bundesgericht hielt fest, dass Art. 15 DSG auf die Art. 28 ff. ZGB verweise und dass in den betreffenden zivilrechtlichen Artikeln sich die Akteneinsicht zwar nicht ausdrücklich im Gesetzestext erwähnt finde, dieser gleichwohl nicht abschliessend zu verstehen sei. Die Akteneinsicht gestützt auf vorsorgliche Massnahmen werde daher keinesfalls durch das Gesetz ausgeschlossen.

Aus der Gerichtspraxis lassen sich auch Angaben zum für die Geltendmachung von Feststellungsansprüchen nach Art. 15 DSG i.V.m. Art. 28a Abs. 1 Ziff. 3 ZGB erforderlichen Feststellungsinteresse (Rechtschutzinteresse) entnehmen. In Änderung seiner Rechtsprechung hielt das Bundesgericht in einem Fall fest, dass die in Art. 28a Abs. 1 Ziff. 3 ZGB vorgesehene Feststellungsklage erhoben werden kann, wenn der Verletzte über ein schutzwürdiges Interesse an der Beseitigung eines fortbestehenden Störungszustandes verfüge, ohne dass es dabei auf die Schwere der Verletzung ankomme[155].

9.3.2 Fazit

Im Überblick ergibt sich somit, dass sich die Bestimmungen des DSG und Art. 28 ff. ZGB (bzw. Art. 328 OR) inhaltlich ergänzen.

Persönlichkeitsverletzungen werden auf Art. 28 ZGB abgestützt; das DSG wird zur Konkretisierung, insbesondere mit Bezug auf die datenschutzrechtlichen Grundsätze herangezogen. Andererseits knüpft Art. 15 DSG an die Widerrechtlichkeit im Sinne von Art. 28 Abs. 2 ZGB an, sodass die weit entwickelte Lehre und Praxis zu dieser Bestimmung auch für die Überprüfung der datenschutzrechtlichen Persönlichkeitsverletzung zum Tragen kommt.

Art. 15 DSG erlangt hingegen als Durchsetzungsrecht nur zusammen mit den Bestimmungen zum Persönlichkeitsschutz, insbesondere Art. 28 Abs. 1 ZGB Bedeutung für die Geltendmachung einer widerrechtlichen Persönlichkeitsverletzung. Eine eigenständige verfahrensrechtliche Bedeutung von Art. 15 DSG als Anspruchsgrundlage konnte nicht festgestellt werden.

9.4 Rechtsansprüche bei der Datenbearbeitung durch Bundesorgane

Zunächst soll der Inhalt des Durchsetzungsrechts nach Art. 25 DSG dargestellt und die einzelnen, darin enthaltenen Anspruchsgrundlagen aufgezeigt werden.

Die daran anschliessend vorzunehmende qualitative Analyse der Rechtsprechung soll in inhaltlicher Hinsicht darüber Auskunft geben, welche materiell- (oder prozess-) rechtlichen Fragen sich bei der Geltendmachung der Durchsetzungerechte nach Art. 25 DSG besonders häufig stellen. Sie hat insbesondere darüber zu informieren, welche gesetzlichen Grundlagen die Bearbeitung

[155] BGE 127 III 481.

von Personendaten durch Bundesorgane typischerweise eben doch zulassen[156] und so der Geltendmachung der Durchsetzungsrechte gestützt auf Art. 25 DSG teils entgegenstehen.

9.4.1 Inhalt des Durchsetzungsrechts (Art. 25 DSG)

Systematik des Gesetzes

Für das Bearbeiten von Personendaten durch Bundesorgane finden Art. 16 ff. DSG Anwendung; die Anspruchsgrundlage für die Geltendmachung von widerrechtlichen Persönlichkeitsverletzungen findet sich in Art. 25 DSG.

Die Bestimmung beinhaltet eine Reihe von Durchsetzungsrechten, die im Folgenden kurz darzustellen sind. Zunächst soll ein Überblick zur Systematik der sich teils wiederholenden Rechte gegeben werden:

- Das Recht auf Berichtigung wird in Art. 5 Abs. 2 und in Art. 25 Abs. 3 DSG erwähnt; gleiches gilt für das Recht auf Sperrung der Bekanntgabe von Daten an Dritte (Art. 20 und 25 DSG).
- Das Recht auf Berichtigung wird in Art. 5 Abs. 2 DSG für die Datenbearbeitung sowohl durch Bundesorgane als auch durch Private verankert, während es in Art. 25 Abs. 3 Bst. a DSG nochmals für Bundesorgane wiederholt wird. Für Bundesorgane ist die letztgenannte Vorschrift als spezifischere Bestimmung massgeblich, wenn auch ihre rechtliche Tragweite Art. 5 Abs. 2 DSG entsprechen dürfte.
- Art. 25 Abs. 3 DSG bezieht sich auf die Sperrung der Bekanntgabe im Falle der widerrechtlichen Bearbeitung und damit auch der widerrechtlichen Bekanntgabe von Personendaten[157]; dagegen regelt Art. 20 DSG die Sperrung der Bekanntgabe von Personendaten, wenn diese grundsätzlich zulässig ist[158].

Berichtigung (Art. 25 Abs. 3 Bst. a DSG)

Art. 25 Abs. 3 Bst. a DSG beinhaltet den Anspruch der betroffenen Person auf Berichtigung unrichtiger Daten. Jedes Daten bearbeitende Bundesorgan hat sich von der Richtigkeit der Daten

---

156 Art. 17 DSG.

157 Z.B. A-7368/2006; bestätigt durch BGer in 1C 225/2007. Voraussetzung für die z.B. Vernichtung von Personendaten ist, dass diese vom verantwortlichen Bundesorgan überhaupt nicht – oder nicht mehr – bearbeitet werden dürfen (Art. 25 DSG). Es geht einmal um jene Fälle, in denen die Widerrechtlichkeit dadurch begründet ist, dass die Daten überhaupt bearbeitet werden. Das ist namentlich der Fall, wenn die Daten ohne ausreichende gesetzliche Grundlage gemäss Art. 17 DSG bearbeitet werden. Aber auch, wenn die Bearbeitung der Daten zur Erfüllung der Aufgaben des verantwortlichen Bundesorgans nicht erforderlich ist oder einen unverhältnismässigen Eingriff in die Privatsphäre des Betroffenen darstellt. Stellen sich die Daten als unrichtig heraus oder sind sie auf widerrechtliche Art und Weise beschafft worden, kann dies ebenfalls die Widerrechtlichkeit nach sich ziehen; A-7368/2006; bestätigt durch BGer in 1C 225/2007.

158 Art. 20 DSG gewährt ein Abwehrrecht gegen die Bekanntgabe von Personendaten durch das verantwortliche Bundesorgan auch in denjenigen Fällen, in denen die Bekanntgabe grundsätzlich zulässig ist. Vor diesem Hintergrund wird ersichtlich, dass die in Art. 25 DSG niedergelegten Ansprüche nicht eingeschränkt werden können (geht es doch um widerrechtliche Bearbeitungen), während dies bei Art. 20 DSG sehr wohl der Fall sein kann.

zu vergewissern und muss diese vernichten bzw. korrigieren, falls sie unrichtig oder unvollständig sind.

Voraussetzung für die Begründetheit des Berichtigungsanspruchs sind die Unrichtigkeit der bearbeiteten Daten und die Richtigkeit derjenigen, die gemäss dem Antrag des Gesuchstellers die unrichtigen Daten ersetzen sollen. Jede noch so nebensächliche Unrichtigkeit ist zu berichtigen.

Das die Daten bearbeitende Bundesorgan kann weder einen Rechtfertigungsgrund geltend machen, noch das schutzwürdige Interesse der betroffenen Person bestreiten bzw. ein eigenes überwiegendes Interesse anführen. Daraus folgt, dass der Berichtigungsanspruch ausnahmslos und uneingeschränkt gilt. Der Nachweis der Unrichtigkeit bzw. der Beweis der Richtigkeit obliegt der betroffenen Person.

Ist der Berichtigungsanspruch begründet, müssen die entsprechenden Daten durch die Berichtigung in Übereinstimmung mit der Wirklichkeit gebracht werden. Grundsätzlich sind verschiedene Arten von Berichtigungen denkbar, z.B. eine Veränderung durch Umgestaltung der Daten, eine teilweise oder ganze Löschung oder eine Hinzufügung von ergänzenden oder neu erhobenen Daten.

Bei der Berichtigung von unrichtigen Daten dürfen keine Kostenbeiträge bei der betroffenen Person erhoben werden.

Die entsprechende Berichtigung, welche jederzeit verlangt werden kann und damit keiner Frist unterliegt[159], ist durch den Datenbearbeiter innerhalb einer angemessenen Frist vorzunehmen. Eine 30-tägige Frist wird sich im Regelfall analog zum Auskunftsrecht als angemessen erweisen.

Der Anspruch auf Berichtigung ergibt sich aus dem Grundsatz der Datenqualität[160]. Damit wird ersichtlich, dass die Bundesorgane auch unabhängig von der Geltendmachung eines Anspruchs auf Berichtigung zur Korrektur unrichtiger Daten verpflichtet sind. Die Richtigkeit von Personendaten ist demnach von Amtes wegen zu prüfen[161].

Kommt das verantwortliche Bundesorgan dieser Pflicht nicht oder nur ungenügend nach, so ist die weitere Bearbeitung der betreffenden Daten widerrechtlich und begründet einen Unterlassungs- und Berichtigungsanspruch gemäss Art. 25 Abs. 1 Bst. a DSG.

Sperrung der Bekanntgabe (Art. 25 Abs. 1 und Abs. 3 Bst. a DSG)

Art. 25 Abs. 1 Bst. a und Abs. 3 Bst. a DSG sehen einen Anspruch auf Sperrung der Bekanntgabe einer widerrechtlichen Datenbearbeitung vor[162].

Anspruchsberechtigt ist jede Person, die ein schutzwürdiges Interesse hat[163]. Dieses liegt in der Regel bereits dann vor, wenn die widerrechtliche Bearbeitung von Daten nach Ansicht des Gerichts gegeben ist[164].

159 BGer 1A.295/2005,Urteil vom 29. März 2006.
160 Art. 5 DSG.
161 Epiney/Zbinden/Civitella 2009: 54 f.
162 Hingegen richtet sich die Sperrung der Bekanntgabe rechtmässig bearbeiteter Daten nach Art. 20 DSG.
163 Art. 25 Abs. 1 DSG.

Bekanntmachungsansprüche (Art. 25 Abs. 1 Bst. c DSG; Art. 25 Abs. 2 DSG; Art. 25 Abs. 3 Bst. b DSG)

Art. 25 DSG sieht diverse Bekanntmachungsansprüche vor, die unter folgenden Voraussetzungen geltend gemacht werden können:

- Die Widerrechtlichkeit der Datenbearbeitung kann gerichtlich festgestellt werden (Art. 25 Abs. 1 Bst. c DSG). Ein solcher Feststellungsanspruch setzt voraus, dass ein entsprechendes Feststellungsinteresse besteht[165].
- In all jenen Fällen, in denen die Richtigkeit von Personendaten nicht bewiesen werden kann, hat das Bundesorgan bei den Daten einen entsprechenden Bestreitungsvermerk anzubringen (Art. 25 Abs. 2 DSG)[166].
- Auf Antrag des Gesuchstellers hat das entsprechende Bundesorgan den im Rahmen des Art. 25 DSG getroffenen Entscheid (z.B. eine Berichtigung oder Vernichtung von Daten) Dritten mitzuteilen oder zu veröffentlichen (Art. 25 Abs. 3 Bst. b DSG).

Sonstige Ansprüche im Zuge einer widerrechtlichen Bearbeitung

Schliesslich ist noch auf weitere Ansprüche hinzuweisen, die im Zusammenhang mit einer widerrechtlichen Datenbearbeitung geltend gemacht werden können:

Das widerrechtliche Bearbeiten von Personendaten ist zu unterlassen (Art. 25 Abs. 1 Bst. a DSG)[167].

Die Folgen eines widerrechtlichen Bearbeitens sind zu beseitigen (Art. 25 Abs. 1 Bst. b DSG). Die betroffene Person kann insbesondere das bereits erwähnte Recht auf Mitteilung oder Veröffentlichung des entsprechenden Entscheids geltend machen.

In Betracht kommen auch etwa Schadensersatz- oder Genugtuungsansprüche, die jedoch auf der Grundlage der Staatshaftung[168] bzw. des Verantwortlichkeitsgesetzes[169] geltend zu machen sind.

Adressat des Art. 25 DSG ist das verantwortliche Bundesorgan[170].

---

164 Vgl. dazu Urteil Nr. 02/99 der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 16. Oktober 2000 (=VPB 66.51); Urteil Nr. 01/00 der Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 22. Dez. 2000. Im Falle einer Bearbeitung von Personendaten, liegt gleichermassen ein Eingriff in das Grundrecht auf „informationelle Selbstbestimmung" vor; BGE 120 Ia 147 E. 2a. Insofern dürfte in aller Regel im Falle einer widerrechtlichen Datenbearbeitung das hier – wie auch etwa in Art. 25 Abs. 2 VwVG oder Art. 89 Abs. 1 Bst. c BGG – für das Vorliegen eines schutzwürdigen Interesses vorausgesetzte aktuelle rechtliche oder tatsächliche Interesse zu bejahen sein.

165 Zum Feststellungsinteresse bei der Geltendmachung von Persönlichkeitsverletzungen durch Private BGE 127 III 481; vgl. Ziffer 9.2.2.

166 Diese Pflicht besteht von Amtes wegen; Urteil Nr. 6/01 vom 7. April 2003 (=VPB 67.73). Zu Fragen der Beweislast im Zusammenhang mit einem Bestreitungsvermerk Urteil Nr. 06/06 der Eidgenössischen Daten- und Öffentlichkeitskommission vom 24. August 2006.

167 Auch hier handelt es sich nicht nur um ein Recht auf Antrag, vielmehr muss die Unterlassung der widerrechtlichen Datenbearbeitung von Amtes wegen beachtet werden.

168 Art. 146 BV.

169 Bundesgesetz vom 14. März 1958 über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten (Verantwortlichkeitsgesetz); SR 170.32.

Das Verfahren der Ausübung der in Art. 25 DSG garantierten Kontrollrechte richtet sich nach dem Verwaltungsverfahrensgesetz[171]. Die Verfügungen des Bundesorgans können beim Bundesverwaltungsgericht angefochten werden[172].

9.4.2 Qualitative Analyse: Überblick

Wie die quantitative Analyse zeigen konnte, ist Art. 25 DSG Gegenstand einiger Urteile der höheren Gerichte. Allerdings beziehen sich die meisten Begehren auf die Berichtigung unrichtiger Daten. Soweit es dagegen um die Zulässigkeit einer Datenbearbeitung als solche geht, steht in der Regel die Existenz einer ausreichenden gesetzlichen Grundlage (Art. 17 Abs. 1 DSG) zur Debatte, die hier kurz betrachtet werden soll.

9.4.3 Zulässigkeit der Datenbearbeitung gestützt auf eine gesetzliche Grundlage im Sinne von Art. 17 Abs. 1 DSG

Zur Frage der Zulässigkeit der Datenbearbeitung gestützt auf die gesetzliche Grundlage ergeben sich verschiedene typische Fallgruppen, die sich insbesondere auf das Verhältnis zwischen Patient, Arzt und Versicherer beziehen. In diesem Zusammenhang ist auf die Unterscheidung der Fallgruppen nach Personendaten[173] einerseits und besonders schützenswerten Personendaten andererseits[174] zurückzukommen.

Das Bundesgericht hatte sich beispielsweise mit einem Fall auseinander zu setzen, bei dem ein ehemaliger Bediensteter des Bundes wegen unverschuldeter Auflösung seines Dienstverhältnisses eine Rente bezog. Diese Rente wurde jedoch den Steuerbehörden gegenüber nicht deklariert. Die daraufhin von der Steuerbehörde konsultierte Beamtenpensionskasse und das Amt für berufliche Vorsorge des betreffenden Kantons verweigerten in der Folge die Bekanntgabe der Auszahlungsadresse der Rente. Dagegen erhob schliesslich die eidgenössische Steuerverwaltung (damals) Verwaltungsgerichtsbeschwerde[175].

Für die Zulässigkeit der Datenbearbeitung – i.c. für die Weitergabe der Daten durch das kantonale Amt für berufliche Vorsorge[176] ist eine gesetzliche Grundlage erforderlich (Art. 17 Abs. 1 DSG). Die erforderliche gesetzliche Grundlage sah das Bundesgericht im Bundesgesetz über die

---

170 Im Gegensatz zu Art. 20 DSG ist das Recht auf Sperrung der Bekanntgabe nach Art. 25 DSG – wie auch die anderen in Art. 25 DSG formulierten Ansprüche – keinen Schranken unterworfen, so dass dem Anspruch immer dann stattzugeben ist, wenn eine widerrechtliche Datenbearbeitung vorliegt.

171 Art. 25 Abs. 4 DSG.

172 Vorher müssen allerdings durch andere Bundesgesetze vorgeschriebene Einsprach- und Beschwerdemöglichkeiten auf Verwaltungsebene ausgeschöpft worden sein.

173 Art. 17 Abs. 1 DSG.

174 Art. 17 Abs. 2 DSG.

175 Bundesgericht 2A.96/2000, Urteil vom 25. Juli 2001.

176 Die kantonalen Ämter für die berufliche Vorsorge gelten als Bundesorgan im Sinne von Art. 3 Bst. h DSG, weil sie Behördenstatus haben und mit öffentlichen Aufgaben des Bundes betraut sind.

direkte Bundessteuer[177], sodass nach der Ansicht des Gerichts die Auskunft zur Auszahlung der Rente aus Gründen des Datenschutzes nicht verweigert werden konnte[178].

In einem weiteren Fall vor dem Bundesverwaltungsgericht stellte sich die Frage, ob die Überwachung der Landesgrenzen durch Drohnenflüge mit den Bestimmungen des DSG vereinbar ist[179].

Das Bundesverwaltungsgericht nahm dabei zuerst kurz zum Begriff der Personendaten Stellung und führte aus, dass unter Personendaten alle *Angaben* zu verstehen seien, die sich auf eine bestimmte oder bestimmbare Person beziehen[180]. Unter Angaben sei jede Art von Information zu verstehen, die auf Vermittlung oder Aufbewahrung von Kenntnissen ausgerichtet sei. Unerheblich sei auch, ob eine Aussage als Zeichen (analog, digital, alphanumerisch oder numerisch), Wort, Bild, Ton oder Kombinationen aus diesen (z.B. Videoaufnahme mit Untertitel) festgehalten sei und auf welcher Art von Datenträger (Papier, Film, elektronische oder optoelektronische Datenträger usw.) die Informationen gespeichert seien. Das Datenschutzgesetz sei demnach auf den durch die Eidgenössische Zollverwaltung veranlassten Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten anzuwenden[181].

Hinsichtlich der für die Datenbearbeitung durch Bundesorgane erforderlichen gesetzlichen Grundlage[182] führte das Bundesverwaltungsgericht aus, dass Art. 1 Bst. a des Zollgesetzes (ZG)[183] u.a. die Überwachung und die Kontrolle des Personen- und Warenverkehrs über die Zollgrenze regle. Nach Art. 108 Abs. 1 Bst. a ZG kann die Zollverwaltung automatische Bildaufnahme- und Bildaufzeichnungsgeräte sowie andere Überwachungsgeräte einsetzen, um unerlaubte Grenzübertritte oder Gefahren für die Sicherheit im grenzüberschreitenden Verkehr frühzeitig zu erkennen. Aufgrund der gesetzlichen Grundlage in Art. 108 ZG hielt die Vorgehensweise der Zollverwaltung nach der Ansicht des Bundesverwaltungsgerichts soweit auch vor dem Datenschutzgesetz stand[184].

Die Gerichte gehen damit von einem weiten Begriff von Personendaten und auch von Bearbeitungen aus, sodass (möglichst) viele Sachverhaltskonstellationen auch unter dem Gesichtswinkel des Datenschutzgesetzes beurteilt werden können. Dadurch geht spezifisch auch das Erfordernis hervor, – dieses ergibt sich auch aus dem Grundsatz der Rechtmässigkeit – dass für sämtliches Handeln der Behörden, das die Bearbeitung von Personendaten betreffen könnte, eine gesetzliche Grundlage vorzusehen ist.

---

177 Bundesgesetzes vom 14. Dezember 1990 über die direkte Bundessteuer (DBG, SR 642. 11).
178 BGer 2A.96/2000, Urteil vom 25. Juli 2001. Das Bundesgericht qualifizierte in diesem Urteil Steuerdaten wiederum nicht als besonders schützenswerte Daten im Sinne von Art. 3 Bst. c DSG; sodass für deren Bearbeitung kein Gesetz im formellen Sinne erforderlich gewesen wäre.
179 Bundesverwaltungsgericht A-2482/2007.
180 Art. 3 Bst. a DSG.
181 Bundesverwaltungsgericht A-2482/2007.
182 Art. 17 Abs. 1 DSG.
183 Zollgesetz (ZG) vom 18. März 2005; SR 631.0.
184 Bundesverwaltungsgericht A-2482/2007.

9.4.4 Bearbeitung besonders schützenswerter Personendaten i.S.v. Art. 17 Abs. 2 DSG

KVG und UVG als spezialgesetzliche Bestimmungen

Die Frage der genügenden gesetzlichen Grundlage für die Zulässigkeit der Bearbeitung von besonders schützenswerten Personendaten durch Bundesorgane[185] stellte sich dem Bundesgericht in einem Fall, wo sich ein Vertrauensarzt einer Krankenversicherung an einen externen Berater – ebenso ein Vertrauensarzt – wandte und ihm zu seiner Beratung das Dossier eines Patienten übermittelte.

Zunächst war festzustellen, dass es sich beim Versicherer um ein Bundesorgan im Sinne des Gesetzes handelte, da dieser mit öffentlichen Aufgaben des Bundes betraut ist; dasselbe gilt für den Vertrauensarzt[186]. Vor dem Bundesgericht stellte sich sodann die Frage der Rechtmässigkeit bzw. der Zulässigkeit der Weiterleitung des medizinischen Dossiers des Versicherten durch den Vertrauensarzt an einen externen Spezialisten ohne Einverständnis oder vorgängige Information des Versicherten[187].

Ein medizinisches Dossier mit Informationen über die Gesundheit des Patienten enthält besonders schützenswerte Daten[188], sodass für deren Bearbeitung – i.c. ging es um die Weiterleitung von Daten – ein Gesetz im formellen Sinne erforderlich ist (Art. 17 Abs. 2 DSG).

Die erforderliche formell-gesetzliche Grundlage fand das Bundesgericht in Art. 84 und 84a des Bundesgesetzes über die Krankenversicherung (KVG)[189]. Subsidiär hätten auch die Bestimmungen für Mitteilungen an Dritte nach Art. 19 DSG und die Ausnahmen von Art. 19 Abs. 1 Bst. b bis d DSG einschlägig sein können. Vorliegend zur Anwendung kam die spezialgesetzliche Regelung des Art. 84a KVG; die Weitergabe des Patientendossiers war damit in einem Gesetz im formellen Sinne vorgesehen und zulässig[190].

In einem weiteren, sehr ähnlich gelagerten Verfahren setzte sich das Bundesgericht[191] mit der Frage auseinander, ob eine genügende gesetzliche Grundlage[192] die Datenbearbeitung durch ein Bundesorgan – i.c. wiederum eine Krankenversicherung[193] – begründen konnte. Der betreffende Krankenversicherer verlangte zwecks Durchführung einer Wirtschaftlichkeitskontrolle in Alters- und Pflegeheimen die Herausgabe von Unterlagen mit Patientendaten, welche die Grundlage für die Pflegebedarfseinstufung bildeten.

Wie bereits angeführt, dürfen besonders schützenswerte Personendaten, wozu namentlich Daten über die Gesundheit gehören[194], und Persönlichkeitsprofile von Krankenversicherern nur unter

185 Art. 17 Abs. 2 DSG.
186 Art. 3 Bst. h DSG.
187 BGE 131 II 413.
188 Art. 3 Bst. c Ziff. 2 DSG.
189 Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG); SR 832.10.
190 BGE 131 II 413. Der Vertrauensarzt bleibe aber – so das Bundesgericht weiter – im Sinne des Verhältnismässigkeitsprinzips verpflichtet, sich unter Achtung der Persönlichkeitsrechte des Versicherten auf die für den beabsichtigten Zweck notwendigen Daten zu beschränken.
191 BGE 133 V 359.
192 Art. 17 Abs. 1 DSG.
193 Krankenversicherer gelten als Bundesorgane im Sinne von Art. 2 Abs. 1 Bst. b und Art. 3 Bst. h DSG.
194 Art. 3 Bst. c Ziff. 2 DSG.

einschränkenden Voraussetzungen bearbeitet werden, dies namentlich wenn ein Gesetz im formellen Sinne es ausdrücklich vorsieht[195].

Art. 84 und 84a KVG begründeten auch für diesen Fall eine eigenständige Regelung des Datenschutzes in der Krankenversicherung. Nach Art. 84 KVG sind die mit der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes betrauten Organe – typischerweise die Krankenversicherer – befugt, auch besonders schützenswerte Personendaten zu bearbeiten, falls diese benötigt werden, um die ihnen übertragene Aufgaben wahrzunehmen, wie z.B. gewisse Leistungsansprüche zu beurteilen[196].

Die Datenbearbeitung im Bereich der Krankenversicherung richtet sich demnach in erster Linie nach diesen spezialgesetzlichen Bestimmungen, welche dem Datenschutzgesetz als sowohl neuere als auch speziellere Bestimmungen vorgehen. Ist eine Datenbearbeitung nach diesen Bestimmungen rechtmässig, besteht nach dem Bundesgericht kein Raum, sie gestützt auf das DSG für unrechtmässig zu erklären[197]. Am Beispiel dieser Erwägung verdeutlicht sich das starke Gewicht, das einer vorliegenden spezialgesetzlichen Bestimmung, welche die Datenbearbeitung zulässt, zukommen kann.

In einem weiteren Verfahren hatte sich das Eidgenössische Versicherungsgericht[198] mit der Frage zu befassen, ob Art. 42 Abs. 3 und 4 KVG ebenfalls eine genügende gesetzliche Grundlage im Sinne von Art. 17 Abs. 2 DSG für die Weitergabe von Patientendaten vom behandelnden Arzt an den Vertrauensarzt des Versicherers beinhalteten. Art. 42 Abs. 3 und 4 KVG statuieren eine Pflicht des Versicherten, den Versicherern alle Angaben weiter zu leiten, welche diese zur Berechnung der Vergütung und zur Überprüfung der Wirtschaftlichkeit der Leistungen benötigen.

In Art. 42 Abs. 3 und 4 KVG sowie Art. 84 und 84a KVG sah das Eidgenössische Versicherungsgericht die für die Datenbearbeitung erforderliche hinreichende gesetzliche Grundlage im Sinne von Art. 17 Abs. 2 DSG für die Beschaffung von Patientendaten vom Leistungserbringer vorliegen. Dabei bezwecke die Institution des Vertrauensarztes im Sinne von Art. 57 KVG im Wesentlichen die Garantie der Persönlichkeitsrechte des Versicherten gegenüber dem Versicherer. Der Versicherer war damit aus datenschutzrechtlicher Sicht berechtigt, die entsprechenden Unterlagen z. Hd. seines Vertrauensarztes herauszuverlangen[199].

In einem weiteren gleich gelagerten Fall – diesmal mit Bezug auf einen Zahnarzt – stellte sich wiederum die Frage, ob eine Krankenversicherung zur Kostenübernahme Einsicht in den Krankenbericht haben darf. Das Bundesgericht führte dazu aus, dass die Leistungserbringer den Vertrauensärzten diejenigen Unterlagen herausgeben müssen, die notwendig sind, um die Leistungspflicht gemäss Art. 57 KVG zu beurteilen. Das Krankenversicherungsgesetz trage dem DSG genügend Rechnung, indem Art. 84 KVG den Vertrauensärzten verbiete, sich mehr Informationen zu beschaffen als in einem formellen Gesetz vorgesehen ist[200]. Auch wenn die Datenbeschaf-

195 Art. 17 Abs. 2 DSG.
196 Art. 84 Bst. c KVG.
197 BGE 133 V 359, 363, 365.
198 Eidgenössisches Versicherungsgericht K 7/05, Urteil vom 18. Mai 2006.
199 Eidgenössisches Versicherungsgericht K 7/05, Urteil vom 18. Mai 2006.
200 Art. 17 Abs. 2 DSG.

fung im Rahmen des Krankenversicherungsgesetzes auf das Notwendigste beschränkt werden müsse, entbinde dies die Leistungserbringer nicht von der Pflicht, den Vertrauensärzten Zugang zu den für die Erfüllung ihrer Aufgaben objektiv notwendigen Informationen zu gewähren. Im vorliegenden Fall waren die verlangten Unterlagen für die Beurteilung der Leistungspflicht der Kasse nach Meinung des Gerichts notwendig. Weder der Versicherte noch der behandelnde Zahnarzt durften daher die Herausgabe verweigern[201].

Auch das Bundesverwaltungsgericht hatte sich zu den Anforderungen an eine formell-gesetzliche Grundlage für die Zulässigkeit einer Datenbearbeitung im Bereich der Krankenversicherung zu äussern, und zwar für die tarifvertragliche Vereinbarung der systematischen Weitergabe der Diagnose durch den Leistungserbringer an den Versicherer im Rahmen der Eintrittsmeldung und der Rechnungsstellung[202].

Art. 84 Bst. c KVG erlaubt es den mit der Durchführung des Gesetzes betrauten Krankenversicherern, Personendaten einschliesslich besonders schützenswerter Personendaten zu bearbeiten, die sie benötigen, um Leistungen zu berechnen. Gemäss Art. 84a Abs. 1 Bst. a KVG dürfen ferner Organe, die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des KVG betraut sind, Daten anderen, ebenfalls im erwähnten Sinne mit den Belangen des KVG betrauten Organen, bekannt geben.

Hinsichtlich der Weitergabe der Diagnose im Rahmen der Eintrittsmeldung erschien damit – unter Vorbehalt der vorliegend erst im Rahmen der Verhältnismässigkeit zu prüfenden Voraussetzung, dass die Diagnose im Sinne des Gesetzes benötigt wird – eine formell-gesetzliche Grundlage gegeben. Aufgrund von Art. 42 Abs. 3 KVG müsse – spezialgesetzlich zu den oben erwähnten Bestimmungen – der Leistungserbringer „dem Schuldner eine detaillierte und verständliche Rechnung zustellen [und] alle Angaben machen, die er benötigt, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können." Nach Art. 42 Abs. 5 KVG schliesslich ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur dem Vertrauensarzt des Versicherers bekannt zu geben. Insgesamt sei – so die Feststellung des Bundesverwaltungsgerichts – Art. 42 Abs. 3 und 4 KVG, in Verbindung mit Art. 84 KVG und 84a KVG als genügende formell-gesetzliche Grundlage für die tarifvertragliche Vereinbarung der systematischen Weitergabe der Diagnose und des Eingriffscodes mit der Rechnungsstellung zu erachten[203].

Das Bundesgericht hatte sich auch mit einem Fall auseinanderzusetzen, bei dem ein Beschwerdeführer die Entfernung eines ärztlichen Gutachtens aus den Akten seines Versicherers verlangte[204].

Dabei wurde ausgeführt, dass gemäss Art. 96 Bst. b des Bundesgesetzes über die Unfallversicherung (UVG)[205] die mit der Durchführung des Unfallversicherungsgesetzes betrauten Organe befugt seien, Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten, falls sie diese benötigten, um Leistungen zu berechnen, zu gewähren und mit Leistungen anderer So-

201 K 18/00, Urteil des Eidgenössischen Versicherungsgerichts vom 27. Januar 2004.
202 BVerwG C-6570/2007. Der Entscheid betrifft das Vorverfahren zum oben erwähnten BGE 133 V 359.
203 Die Beschwerde wurde schliesslich aufgrund der Verletzung des Verhältnismässigkeitsgrundsatzes abgewiesen.
204 BGr 8C 550/2007, Urteil vom 12. März 2008.
205 Bundesgesetz vom 20. März 1981 über die Unfallversicherung (UVG); SR 832.20. Damals: Art. 97a Bst. b UVG.

zialversicherungen zu koordinieren[206]. Für die Datenbearbeitung hatte somit nach Ansicht des Bundesgerichts eine gesetzliche Grundlage bestanden, weshalb sie – nach Auffassung des Gerichts – aus datenschutzrechtlicher Sicht nicht zu beanstanden war[207].

In einem weiteren Fall vor dem Bundesverwaltungsgericht hatte der Beschwerdeführer aufgrund einer psychischen Erkrankung seine Stelle in der Bundesverwaltung verloren und wollte deswegen Schadenersatz aus Staatshaftung geltend machen[208]. Im Laufe des Verfahrens soll unter anderem ein Vertreter des betroffenen Bundesamtes direkt den Hausarzt des Beschwerdeführers kontaktiert haben, um Näheres über dessen Gesundheitszustand zu erfahren. Es stellte sich die Frage, ob eine Rechtsgrundlage für die direkte Kontaktnahme mit dem Hausarzt durch Bundesangestellte besteht[209]. Für das Personalrecht des Bundes findet sich diese Grundlage in Art. 28 BPG i.V.m. Art. 11 der Bundespersonalverordnung vom 3. Juli 2001 (BPV), wo ein spezieller ärztlicher Dienst der Bundesverwaltung geschaffen wird. Der Kontakt mit den behandelnden Ärzten eines Mitarbeiters hat folglich durch diesen zu erfolgen. Eine direkte Kontaktnahme der Bundesverwaltung mit dem Hausarzt wurde mangels formell gesetzlicher Grundlage als unzulässig qualifiziert[210].

In einem länger andauernden Rechtsstreit[211] verlangte der Beschwerdeführer gestützt auf Art. 25 Abs. 3 Bst. a DSG die Vernichtung eines medizinischen Gutachtens aus dem Jahr 1959 bei der SUVA. Das Gutachten selbst war bei der SUVA nicht mehr vorhanden, jedoch war diese in der Lage, dem Bundesverwaltungsgericht zur Beurteilung des Falles eine Kopie desselben zur Verfügung zu stellen. Der Beschwerdeführer beantragte auch die Vernichtung dieser Kopie[212].

Das Bundesverwaltungsgericht führte zunächst dazu aus, dass unter den Begriff des Bearbeitens nach Art. 3 Bst. e DSG nicht nur die Erstellung eines Gutachtens, sondern in gleicher Weise auch dessen Aufbewahrung oder Archivierung falle[213].

Voraussetzung für die Vernichtung von Personendaten nach Art. 25 Abs. 3 Bst. a DSG sei es – so das Bundesverwaltungsgericht weiter –, dass diese vom verantwortlichen Bundesorgan nicht (oder nicht mehr) bearbeitet werden dürfen. Das sei namentlich der Fall, wenn die Daten ohne ausreichende gesetzliche Grundlage[214] bearbeitet werden[215].

Mit dem Gutachten und der Überweisung einer Kopie desselben an das Bundesverwaltungsgericht habe die SUVA besonders schützenswerte Personendaten des Beschwerdeführers bearbeitet[216]. Diese dürfen jedoch grundsätzlich nur bearbeitet werden, wenn ein Gesetz im formellen Sinne dies ausdrücklich vorsehe[217]. Die vom Datenschutzgesetz verlangte Rechtsgrundlage finde

206 BGr 8C 550/2007, Urteil vom 12. März 2008.
207 BGr 8C 550/2007, Urteil vom 12. März 2008.
208 Bundesverwaltungsgericht A-5748/2008.
209 Art. 3 Bst. c Ziff. 2 i.V.m. Art. 17 Abs. 2 DSG.
210 Bundesverwaltungsgericht A-5748/2008.
211 Vgl. auch BGer in 8C_941/2008.
212 BVerwG A-6067/2008, Urteil vom 30. März 2009.
213 BVerwG A-6067/2008, Urteil vom 30. März 2009.
214 Art. 17 DSG.
215 BVerwG A-6067/2008, Urteil vom 30. März 2009.
216 Art. 3 Bst. c Ziff. 2 DSG.
217 Art. 17 Abs. 2 DSG.

sich für den Bereich der Unfallversicherung in den Art. 96 f. des Unfallversicherungsgesetzes, die spezifische Regelungen für das „Bearbeiten von Personendaten“[218] beziehungsweise die „Datenbekanntgabe“[219] regeln – und die als spezialgesetzliche Bestimmungen den allgemeinen Regelungen im Datenschutzgesetz vorgehen. Die Archivierung des Gutachtens erfolgte gestützt auf die spezialgesetzlichen Bestimmungen rechtens[220].

Dagegen war jedoch nach Ansicht des Bundesverwaltungsgerichts die Einholung einer Kopie des Gutachtens aus dem Jahre 1959 nach Art. 96 UVG und auch im Zusammenhang mit dem datenschutzrechtlichen Verfahren nicht erforderlich. Die Datenbearbeitung war damit – unabhängig von der Richtigkeit der bearbeiteten Daten – widerrechtlich im Sinne von Art. 25 Abs. 1 Bst. a DSG i.V.m. Art. 4 Abs. 1 und 2 DSG. Die Kopie war – nach Rücksendung der Akten vom BVGer an die SUVA – gestützt auf Art. 25 Abs. 3 Bst. a DSG zu vernichten[221].

Die Bearbeitung von besonders schützenswerten Personendaten war auch in anderen als in den medizinversicherungsrechtlichen Fällen zu prüfen. In BGE 122 I 360 verlangten die Beschwerdeführer bei der Erziehungsdirektion eines Kantons Einsicht in die über sie erstellten Datenblätter betreffend ihre Beziehung zum Verein für Psychologische Menschenkenntnis (VPM). Die Erziehungsdirektion gewährte den Beschwerdeführern Einsicht in die Datenblätter und eröffnete ihnen, dass Datenblätter und Korrespondenz im Zusammenhang mit dem Einsichtsgesuch in die entsprechenden ordentlichen Personaldossiers abgelegt wurden. Eine bestimmte Quelle, die auf einem Teil der Datenblätter angegeben war, wurde jedoch abgedeckt. Dagegen erhoben die Beschwerdeführer Staatsrechtliche Beschwerde beim Bundesgericht[222].

Da die systematische Erhebung von besonders schützenswerten Daten einzig auf die Vereinszugehörigkeit abstellte und keinen unmittelbaren Zusammenhang mit dem kantonalen Schulbetrieb aufwies, war sie – so die Ausführungen des Bundesgerichts – für die Betroffenen nicht voraussehbar. Für die Bearbeitung solcher Daten wäre eine klare gesetzliche Grundlage erforderlich gewesen, die mit der nötigen Bestimmtheit geregelt hätte, unter welchen Voraussetzungen und zu welchem Zweck die Mitgliedschaft von Angestellten des Kantons in politischen oder weltanschaulichen Vereinen registriert hätte werden dürfen, welcher Personenkreis hätte erfasst werden dürfen, wem derartige Informationen hätten bekanntgegeben werden dürfen und unter welchen Voraussetzungen die Daten wieder gelöscht hätten werden müssen.

Die Beschaffung, Aufbewahrung und Bearbeitung persönlicher, der Öffentlichkeit sonst nicht zugänglicher Daten könne einen Eingriff in die (nach damals ungeschriebenem Verfassungsrecht als Teil der persönlichen Freiheit geschützte) Geheimsphäre darstellen und berühre die nach Art. 8 Ziff. 1 EMRK geschützte Privatsphäre. Einschränkungen der persönlichen Freiheit seien zulässig, wenn sie auf einer gesetzlichen Grundlage beruhen, im öffentlichen Interesse liegen, verhältnismässig sind und den Kerngehalt des Grundrechts nicht verletzen. Die Voraussetzung der gesetzlichen Grundlage war i.c. nicht erfüllt[223].

---

218 Art. 96 UVG.
219 Art. 97 UVG.
220 BVerwG A-6067/2008, Urteil vom 30. März 2009.
221 BVerwG A-6067/2008, Urteil vom 30. März 2009.
222 BGE 122 I 360.
223 BGE 122 I 360.

DSG als Auslegehilfe

In einem weiteren Fall vor dem Eidgenössischen Versicherungsgericht[224], der die Herausgabe von Patientenakten im Rahmen eines kantonalen Schiedsverfahrens in Sozialversicherungsstreitigkeiten betraf, wurde zunächst festgestellt, dass die Personendaten der Patientenkartei einer Arztpraxis grundsätzlich dem durch Art. 28 ZGB geschützten Geheimbereich der betreffenden Patientinnen und Patienten zuzurechnen seien und dass die Weitergabe solcher Daten in der Regel eine Persönlichkeitsverletzung bedeute, die nach Art. 28 Abs. 2 ZGB nur dann nicht widerrechtlich sei, wenn sie durch Einwilligung der Betroffenen, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt sei. Nähere Bestimmungen zum Schutz der Persönlichkeitsrechte enthalte das DSG, welches gemäss Art. 2 Abs. 2 Bst. c jedoch nicht anwendbar sei auf staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren[225].

Eine entsprechende Bestimmung enthalte dagegen § 40 des Gesetzes über das Sozialversicherungsgericht des Kantons Zürich vom 7. März 1993, wonach die Parteien im Verfahren vor dem Schiedsgericht von der Pflicht zur Wahrung des Berufsgeheimnisses entbunden wurden, soweit dies zur Feststellung des Sachverhalts in der streitigen Angelegenheit erforderlich war. Diese spezifisch auf Verfahren zwischen Krankenversicherern und Leistungserbringern gemäss Art. 89 Abs. 1 KVG zugeschnittene Bestimmung stelle – neben Art. 81 Abs. 1 KVG – eine hinreichende gesetzliche Grundlage für die Entbindung der Partei vom Berufsgeheimnis und die Auskunftspflicht gegenüber dem Schiedsgericht dar.

Im vorliegenden Fall hatte das Schiedsgericht demnach zu Recht ergänzende Unterlagen eingefordert[226].

9.4.5 Fälle zur gesetzlichen Grundlage im Sinne von Art. 17 DSG mit Bezug zu Art. 19 DSG

In einem weiteren Verfahren vor dem Bundesverwaltungsgericht[227] ging es um ein Eheschutzverfahren. Die Unfallversicherung des Ehemanns wurde gerichtlich angewiesen, von den künftigen Rentenauszahlungen bis auf weiteres den gleichen Betrag direkt auf ein Konto der Ehefrau zu überweisen. Als die Rentenzahlungen an den Ehemann nicht mehr ausgerichtet wurden, stellte die Unfallversicherung auch die Zahlungen an die Ehefrau ein. Daraufhin ersuchte die Ehefrau die Unfallversicherung um Einsicht in die Unfallakten ihres Ehemannes. Diese wurde ihr verweigert. Im Beschwerdeverfahren war insbesondere die gesetzliche Grundlage für eine Datenbekanntgabe strittig. Es stellte sich die Frage der Rechtsgrundlage für die Einsicht in Versicherungsakten einer Unfallversicherung durch die Ehefrau des Versicherten.

---

224 K 90/01, Urteil des Eidgenössischen Versicherungsgerichts vom 27. November 2001.

225 Auf den vorliegenden Fall nicht anwendbar ist auch das zürcherische Datenschutzgesetz, welches gemäss § 3 Bst. b nicht gilt in hängigen Verfahren der Zivil-, Verwaltungs- und Strafrechtspflege. Massgebend für die Beurteilung der streitigen Rechtsfrage sind die anwendbaren sozialversicherungs- und verfahrensrechtlichen Bestimmungen; ferner sind die strafrechtlichen Vorschriften von Art. 321 StGB zu beachten.

226 K 90/01, Urteil vom 27. November 2001.

227 A-7367/2006 (bezüglich Rechtsweg aufgehoben durch BGer in 8C 192/2008).

Gemäss Art. 19 Abs. 1 DSG dürfen Bundesorgane – zu welchen vorliegend auch die Versicherung zu zählen ist[228] – Personendaten bekannt geben, wenn dafür eine gesetzliche Grundlage im Sinne von Art. 17 DSG besteht. Besonders schützenswerte Personendaten[229] dürfen nur bearbeitet werden, wenn ein formelles Gesetz es ausdrücklich vorsieht[230].

Die fraglichen Akten der Versicherung betreffend den Ehemann beinhalteten besonders schützenswerte Personendaten im Sinne von Art. 3 Bst. c Ziff. 2 DSG. Sowohl Art. 17 DSG (Abs. 2 Bst. a, b und c) als auch Art. 19 DSG (Abs. 1 Bst. a bis d) sehen beim Fehlen einer gesetzlichen Grundlage Ausnahmen vom Erfordernis einer gesetzlichen Grundlage für die Datenbearbeitung resp. -herausgabe vor. Somit war zunächst zu prüfen, ob sich für die beantragte Datenbekanntgabe eine Grundlage in einem Gesetz im formellen Sinne gemäss Art. 17 Abs. 2 DSG finden liesse. Erst anschliessend wäre – sollte keine solche gegeben sein – zu prüfen, ob allenfalls ein Ausnahmetatbestand aus Art. 17 bzw. Art. 19 DSG anwendbar wäre.

Vorliegend ging es um Daten, die von einem Versicherungsunternehmen im Sinne von Art. 68 Abs. 1 Bst. a UVG im Rahmen des Versicherungsverhältnisses (Art. 59 UVG) bearbeitet wurden. In Art. 96 f. UVG finden sich spezifische Informationsbearbeitungs- und Datenschutzregelungen. Art. 97 des Bundesgesetzes über die Unfallversicherung regelt die Datenbekanntgabe. Mit Art. 97 UVG[231] habe der Gesetzgeber die erforderliche formell gesetzliche Grundlage zur Bekanntgabe von besonders schützenswerten Personendaten geschaffen.

Nach Art. 97 Abs. 6 Bst. a UVG dürfen Organe, die mit der Durchführung sowie der Kontrolle oder Beaufsichtigung der Durchführung des Gesetzes betraut sind, Personendaten bekannt geben – sofern kein überwiegendes Privatinteresse besteht. Als zusätzliches Erfordernis muss die betroffene Person im Einzelfall schriftlich eingewilligt haben oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden können. Nach Einschätzung des BVGer wäre die Aktenherausgabe in diesem Fall auch im Interesse des – unauffindbaren – Ehemanns gewesen, weil die Fortsetzung der Rentenzahlung auch in seinem Interesse lag; seine mutmassliche Einwilligung hätte deshalb angenommen werden können. Die Versicherung wäre damit berechtigt, aber nicht verpflichtet gewesen, die Daten bekannt zu geben. Die durch das BVGer vorgenommene Interessenabwägung ergab, dass weder private noch öffentliche Interessen vorlagen, die eine Verweigerung der Einsichtsmöglichkeit rechtfertigen würden. Der Ehefrau war deshalb durch die Unfallversicherung das Einsichtsrecht zu gewähren[232].

In BGE 124 III 170 setzte sich das Bundesgericht mit der Frage auseinander, ob die Auskunftspflicht der Behörden nach Art. 91 Abs. 5 SchKG mit den Bestimmungen des DSG vereinbar sei. Gemäss Art. 91 Abs. 5 SchKG sind Behörden in den Fällen, in denen beim Schuldner eine Pfändung vollzogen wird, im gleichen Umfang auskunftspflichtig wie der Schuldner.

---

228 Vgl. Art. 3 Bst. h DSG.
229 Art. 3 Bst. c DSG.
230 Art. 17 Abs. 2 DSG.
231 Bzw. der Vorgängerregelung: Art. 102a.
232 A-7367/2006 (bezüglich Rechtsweg aufgehoben durch BGer in 8C 192/2008).

Gemäss Art. 19 Abs. 1 Bst. a DSG dürfen Bundesorgane Personendaten nicht nur bekanntgeben, wenn dafür Rechtsgrundlagen im Sinne von Art. 17 DSG bestehen, sondern auch, wenn die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind. Ein Betreibungsbeamter, der zum Vollzug einer Pfändung schreite, erfülle eine gesetzliche Aufgabe. Er müsse die tatsächlichen Verhältnisse, die zur Ermittlung des pfändbaren Erwerbseinkommens nötig sind, von Amtes wegen abklären.

Aus Art. 91 Abs. 5 SchKG leitet sich demnach unmittelbar die Pflicht der Behörden – insbesondere auch der im Bereich des Sozialversicherungsrechts tätigen Ämter – ab, dem Betreibungsamt Auskunft zu erteilen. Die Bestimmung sei demnach mit den Grundlagen des DSG vereinbar[233].

Auch in Bezug auf die Amtshilfe hatte das Bundesgericht die Anforderungen an die Voraussetzung der gesetzlichen Grundlage zu prüfen. Es hielt fest, dass auch ein völkerrechtlicher Vertrag wie das Doppelbesteuerungsabkommen mit den USA als gesetzliche Grundlage i.S.v. Art. 19 DSG (und damit wohl auch i.S.v. Art. 17 DSG) gelten könne[234].

9.4.6 Fazit

Insgesamt sind in der Rechtsprechung einige Urteile zu verzeichnen, die die Durchsetzungsrechte aus Art. 25 DSG zum Gegenstand hatten, wobei die meisten Begehren Ansprüche auf Berichtigung waren. Auf dieses Recht entfällt die grösste Anzahl geltend gemachter Durchsetzungsansprüche; diese Häufung ist allerdings relativ zu verstehen, denn die Durchsetzungsrechte werden insgesamt selten geltend gemacht.

Beschwerden gestützt auf die Durchsetzungsrechte hatten nur in seltenen Fällen Erfolg; am ehesten Berichtigungsgesuche gestützt auf Art. 25 Abs. 3 Bst. a DSG, jedoch in sachlich konzentrierten Fallkonstellationen (z.B. Bereich Asyl).

Ansonsten stand im Zusammenhang mit der Zulässigkeit der Datenbearbeitung durch Bundesorgane häufig die Frage nach der Existenz einer gesetzlichen Grundlage, deren Reichweite die Gerichte dann jeweils auch im konkreten Fall auszulegen hatten, im Vordergrund. Dabei wird die Existenz einer formell-gesetzlichen Grundlage im Falle der Bearbeitung besonders schützenswerter Personendaten i.S.v. Art. 3 Bst. c DSG jeweils genau geprüft. Insgesamt wird in der Rechtsprechung dem Vorliegen einer spezialgesetzlichen Regelung ein sehr starkes Gewicht eingeräumt; hingegen wird das Verhältnis der spezialgesetzlichen Regelung zu den allgemeinen Bearbeitungsgrundsätzen *des DSG* nicht immer klar dargestellt[235].

[233] Art. 19 Abs. 1 Bst. a DSG.
[234] A-7342/2008.
[235] Vgl. dazu etwa den oben angeführten BGE 133 V 359, 363.

9.5 Geltendmachung der Strafbestimmungen

9.5.1 Anwendung Strafbestimmungen (Art. 34 und 35 DSG)

Es konnten vor dem Bundes- und Bundesverwaltungsgericht drei Fälle gefunden werden, von denen das Verfahren in einem Fall eingestellt wurde[236] und in zwei Fällen vor dem Bundesgericht mit Nichteintreten endete[237].

Die strafrechtlichen Bestimmungen des DSG wurden vor der Eidgenössischen Datenschutz- und Öffentlichkeitskommission, soweit ersichtlich, nicht angerufen.

Die Strafbestimmungen im Sinne des DSG wurden auf kantonaler Ebene in einem bernischen Haftpflichtfall angerufen, in dem es um den Beizug eines ärztlichen Gutachtens ohne Einwilligung des Patienten ging. Vom Vorwurf der Verletzung der gesetzlichen Schweigepflicht wurde der behandelnde Arzt freigesprochen[238].

9.5.2 Fazit

Die Strafbestimmungen des DSG sind in der Gerichtspraxis kaum von Bedeutung.

[236] BGE 122 IV 139.
[237] BGr. 6B 335/2007, Urteil vom 5. Oktober 2007; 8G.75/2003; Urteil vom 5. September 2003.
[238] VGE 218010; Urteil des Verwaltungsgerichts des Kantons Bern vom 09. November 2004.

10 Zusammenfassung und Fazit zu den Durchsetzungsrechten

Dieser Teil der Evaluation befasste sich mit dem ersten zu untersuchenden Wirkungsmechanismus des DSG: den Durchsetzungsrechten, die von den Betroffenen selber in Anspruch genommen werden können. Im Zentrum stand die Frage, inwieweit die im DSG enthaltenen Bestimmungen, mit denen betroffene Personen eine mutmassliche Datenschutzverletzung durch private oder öffentliche Datenbearbeiter vor Gericht geltend machen können, geeignet sind, den Schutz der Persönlichkeitsrechte angemessen zu gewähren. Nachfolgend werden die Befunde aus den drei vorangegangenen Kapiteln zusammengefasst und bilanziert.

10.1 Durchsetzungsrechte des DSG im internationalen Vergleich

Kapitel 7 diskutierte die Durchsetzungsrechte des DSG im internationalen Vergleich. Dabei lässt sich feststellen, dass diesbezüglich eher geringe Unterschiede zwischen den untersuchten Ländern bestehen: Die in der Schweiz bestehenden Durchsetzungsrechte sind auch in den meisten anderen untersuchten Ländern vorhanden. Andere Durchsetzungsrechte als jene der Schweiz finden sich kaum. Die gewichtigste Ausnahme bildet das Widerspruchsrecht der Betroffenen, welches der Gesetzgeber in Deutschland und Österreich vorgesehen hat. Mehrere Länder sehen wie die Schweiz Gerichte als Durchsetzungsinstanzen vor; alternativ wird diese Funktion teilweise auch Datenschutzbehörden selber übertragen. Vereinzelt schliesslich finden sich Klagerechte für Vereine oder die Möglichkeit einer Sammelklage. Einzelne Länder sehen die Möglichkeit von Schadenersatzklagen vor.

10.2 Bekanntheit und Inanspruchnahme der Durchsetzungsrechte

Im achten Kapitel wurde untersucht, wie gut die Bevölkerung die Durchsetzungsrechte kennt, und wie stark sie diese in Anspruch nimmt. Aufgrund der Bevölkerungsbefragung lässt sich festhalten, dass das DSG einer Mehrheit bekannt ist. Allerdings dürfte es sich dabei eher um eine oberflächliche Kenntnis handeln: Nur eine Minderheit von 26% der Befragten ist sich sicher, dass sie als Betroffene bei einer mutmasslichen Verletzung des DSG den Rechtsweg einschlagen können. Ebenso deutet das in der Umfrage berichtete Verhalten in realen und potenziellen Missbrauchssituationen darauf hin, dass der Rechtsweg bei der Bevölkerung wenig bekannt ist bzw. eine geringe Bedeutung aufweist: So würde sich ein beträchtlicher Teil der Befragten im Missbrauchsfall an die Polizei wenden. Nur eine Minderheit gab an, eine Rechtsberatung oder Anwalt zu konsultieren, oder sich ans Gericht zu wenden. Auch die befragten Experten vermuten eine ungenügende Bekanntheit der Durchsetzungsrechte in der Bevölkerung: Nicht nur seien die Rechte an sich nicht oder nur oberflächlich bekannt; darüber hinaus fehle den Betroffenen auch das (juristische) Wissen, wie die Rechte im konkreten Fall anzuwenden und durchzusetzen seien. Dabei wird von einer Überforderung der Bevölkerung gesprochen.

Die Analyse der Rechtsprechung bestätigt den Eindruck, dass die Rechte durch die Betroffenen nur selten in Anspruch genommen werden. Von den 269 überprüften Fällen vor Bundesverwal-

tungsgericht (ab 2007), vor der eidgenössischen Rekurskommission (bis 2006), von den kantonalen Entscheiden und vor Bundesgericht betraf die grösste Anzahl Fälle die Geltendmachung von Einsichtsrechten nach Art. 8 DSG resp. den entsprechenden kantonalen Bestimmungen. Nur ein geringer Anteil der Fälle betraf demgegenüber die Durchsetzungsrechte gemäss Art. 15 und 25 DSG. Die Geltendmachung der Einsichtsrechte blieb vor den kantonalen Instanzen überwiegend ohne Erfolg. Dagegen war gut die Hälfte der vor den höheren Instanzen geltend gemachten Beschwerden erfolgreich. Von den vergleichsweise wenigen Fällen, die sich auf die Durchsetzungsrechte im Sinne von Art. 15 und 25 DSG (oder die entsprechenden kantonalen Bestimmungen) stützten, betrafen die meisten Ansprüche Art. 25 DSG, die sich auf Datenbearbeitungen von Bundesorganen beziehen, und insbesondere Berichtigungsgesuche. Erfolg hatten die Beschwerden gestützt auf die Durchsetzungsrechte nur in seltenen Fällen; am ehesten erfolgreich waren Berichtigungsgesuche gestützt auf Art. 25 Abs. 3 Bst. a DSG (Unterlassung des widerrechtlichen Bearbeitens von Personendaten), jedoch in sachlich konzentrierten Fallkonstellationen (z.B. im Asylbereich). Die durchgeführte Fallrecherche zeigte überdies, dass die Strafbestimmungen des DSG (Art. 34 und 35 DSG) in der Gerichtspraxis kaum eine Bedeutung haben. In inhaltlicher Hinsicht fällt auf, dass vor Gericht keine Fälle vorgebracht wurden, die als typisch für die neuen, intransparenten Konstellationen zwischen Bearbeiter und Betroffenen beschrieben werden könnten. Dies kann nicht überraschen, ist es doch eine Voraussetzung für einen Prozess, dass der Beklagte dem Kläger bekannt ist.

Als mögliche Gründe für die geringe Nutzung des Rechtsweges durch die Betroffenen können neben der bereits erwähnten bescheidenen Kenntnissen über die Rechte an sich und deren Anwendung Überlegungen zum Verhältnis von Kosten und Nutzen vorgebracht werden. Der Nutzen, der aus einer erfolgreichen Inanspruchnahme der Durchsetzungsrechte resultieren kann, wird als gering eingestuft: Es fällt den Betroffenen schwer, den Nutzen eines positiven Urteils genau zu bestimmen; insbesondere ist es kaum möglich, einen entstandenen Schaden zu quantifizieren oder zu beurteilen, welche weiteren Folgen sich aus einer Datenschutzverletzung ergeben können. Spezifisch für den Arbeitsbereich kann erwähnt werden, dass das Vorgehen gegen den Arbeitgeber auf dem Gerichtsweg darüber hinaus mit dem Risiko einer Kündigung verbunden ist.

10.3 Anwendung und Konkretisierung des DSG durch die Gerichte

Die erfolgte Analyse der Rechtsprechung zu ausgewählten Bestimmungen des DSG erlaubt einige Schlussfolgerungen, die im Folgenden kurz dargelegt werden sollen, wobei zwischen dem Auskunftsrecht, der Durchsetzung in Bezug auf Datenbearbeitungen Privater, der Durchsetzung in Bezug auf Datenbearbeitungen von Bundesorganen und, mit Letzterem zusammenhängend, dem Verhältnis des DSG zu anderen (spezialgesetzlichen) Vorgaben zu unterscheiden ist.

10.3.1 Zum Auskunftsrecht

Das Auskunftsrecht des Art. 8 DSG hat sich insgesamt wohl bewährt, so dass es sich nicht aufdrängt, die diesbezüglichen Rechtsgrundlagen zu modifizieren. Insbesondere erschiene es nicht oder allenfalls nur sehr schwer möglich, die Schranken des Auskunftsrechts – insbesondere so-

weit die ihm (möglicherweise) entgegenstehenden öffentlichen oder privaten Interessen betroffen sind – weiter zu präzisieren, da hier letztlich Interessenabwägungen eine entscheidende Rolle spielen, deren Durchführung bzw. Ergebnisse sich einer abstrakt-generellen Regelung letztlich entziehen.

10.3.2 Zur Durchsetzung gegenüber privaten Datenbearbeitern

Art. 15 DSG dürfte kaum eine eigenständige Bedeutung zukommen; letztlich erlangt diese Bestimmung nur zusammen mit Art. 28 ZGB wirklich Bedeutung. Aber auch darüber hinaus spielt Art. 15 DSG in der gerichtlichen Praxis insgesamt eine untergeordnete Rolle. Denn häufig scheuen sich Private, im Falle einer Persönlichkeitsverletzung den Rechtsweg – entsprechend der Grundkonzeption des Art. 15 DSG – zu bestreiten, wohl in erster Linie, weil das Prozess- und Kostenrisiko als unverhältnismässig angesehen wird, eine Überlegung, die wohl insbesondere immer dann zum Tragen kommt, wenn eine widerrechtliche Persönlichkeitsverletzung als nicht „gravierend" angesehen wird und zu keinen materiellen Schäden geführt hat.

Die angedeuteten Defizite implizieren, dass – sozusagen systemimmanent – eine Reihe von widerrechtlichen Persönlichkeitsverletzungen nicht festgestellt und damit ggf. auch bestehen bleiben. Diese Situation ist schon deshalb unbefriedigend, weil auch vermeintlich „harmlose" Persönlichkeitsverletzungen mitunter für die Betroffenen nicht vorhersehbare Konsequenzen entfalten können, ganz abgesehen davon, dass das DSG grundsätzlich davon ausgeht, dass jede widerrechtliche Persönlichkeitsverletzung zu unterbleiben hat.

10.3.3 Zur Durchsetzung gegenüber Bundesorganen und zur Rolle spezialgesetzlicher Regelungen

Art. 25 DSG ist Gegenstand einiger Urteile der höheren Gerichte. Allerdings beziehen sich die meisten Begehren auf die Berichtigung (vermeintlich) unrichtiger Daten. Soweit es um die Zulässigkeit einer Datenbearbeitung als solche geht, steht in der Regel die Existenz einer (ausreichenden) gesetzlichen Grundlage zur Debatte.

In der Gerichtspraxis ist das Vorliegen einer spezialgesetzlichen Bestimmung in der Regel entscheidend für die Zulässigkeit der Datenbearbeitung. Zwar ist im Gesetzgebungsprozess einerseits der EDÖB zur Stellungnahme eingeladen (Art. 31 Abs. 1 Bst. b DSG, vgl. Ziffer 12.7), andererseits werden Gesetzesreformen vom Bundesamt für Justiz auf die Einhaltung übergeordneten Rechts hin kontrolliert (Fachbereich Rechtsetzungsbegleitung); angesichts der fehlenden Verfassungsgerichtsbarkeit gegenüber Bundesgesetzen kann jedoch nicht verwaltungsunabhängig geprüft werden, ob diese spezialgesetzlichen Grundlagen immer auch den verfassungsrechtlichen Anforderungen gerecht werden. Eine entsprechende Überprüfung und Evaluation der spezialgesetzlichen Erlasse würde den Rahmen dieser Untersuchung deutlich sprengen.

In diesem Zusammenhang ist es gleichwohl wichtig, festzuhalten, dass nach der hier vertretenen Ansicht die allgemeinen Grundsätze der Datenbearbeitung grundsätzlich neben der einschlägigen Spezialgesetzgebung anzuwenden sind, weil sie die verfassungsrechtlichen Vorgaben und die Anforderungen der EMRK „konkretisieren" (Maurer-Lambrou/Steiner 2006: 79; N. 3 zu Art. 4

DSG), so dass sie nicht durch spezialgesetzliche Regelungen „unterlaufen“ werden dürfen. M.a.W. sind die datenschutzrechtlichen Grundsätze als jedenfalls zu beachtende Anforderungen an die Datenbearbeitung anzusehen, die durch spezialgesetzliche Vorgaben lediglich präzisiert und weiterentwickelt, jedoch nicht relativiert werden dürfen.

10.4 Gesamtbilanz

Insgesamt lässt sich die Hauptfragestellung dieses Teils, nämlich inwiefern die im DSG verankerten Durchsetzungsrechte den Schutz der Persönlichkeitsrechte ausreichend gewährleisten können, kritisch beantworten: Der Gerichtsweg wird – sieht man vom gelegentlich vorgebrachten Auskunftsrecht ab – kaum in Anspruch genommen, wobei sich diese Tatsache nicht mit einer durchgehend hohen Sensibilität der Datenbearbeiter begründen lässt: Die Ergebnisse der Bevölkerungsbefragung in Bezug auf Missbrauchserfahrungen, die Einschätzung der Experten hinsichtlich der Einhaltung der DSG-Bestimmungen durch Datenbearbeiter sowie die Analyse der Aufsichtstätigkeit des EDÖB (vgl. Ziffern 12.3 und 12.4) liefern empirische Evidenz dafür, dass es in der Praxis zu Verletzungen der Persönlichkeitsrechte der Betroffenen kommt.

TEIL IV: EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER

Dieser Teil der Evaluation befasst sich mit dem Aufsichtsorgan des schweizerischen Datenschutzgesetzes, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Die empirische Untersuchung gliedert sich in zwei grössere Bestandteile. In Kapitel 11 liegt der Fokus auf organisatorischen Aspekten, so insbesondere der institutionellen Stellung und Unabhängigkeit des EDÖB, seinen zentralen Steuerungsprozessen, seinen Ressourcen und der Zusammenarbeit mit anderen Akteuren des Datenschutzes. In Kapitel 12 stehen die wichtigsten Aktivitäten des EDÖB (Aufsicht, Beratung, Information, Stellungnahmen in Rechtsetzungsprozessen) sowie deren Wirkungen im Mittelpunkt. Dabei ist auch zu beachten, inwieweit die Instrumente des EDÖB vor dem Hintergrund der technologischen Herausforderungen und der zunehmenden Internationalität der Datenbearbeitungen insbesondere im Internet noch Wirkung entfalten können. Kapitel 13 fasst die Befunde zusammen und zieht ein Fazit zur Organisation, Strategie und der Wirksamkeit des EDÖB.

Die nachfolgenden Ausführungen stützen sich auf mehrere Informationsquellen, so auf die Aussagen der Interviewpartner (Experten, Interessenvertreter, Datenbearbeiter, Mitarbeitende beim EDÖB) sowie auf diverse Arbeitsunterlagen des EDÖB, auf Daten des Geschäftsverwaltungssystems des EDÖB seit dem Geschäftsjahr 2003/04, auf die Tätigkeitsberichte seit dem Geschäftsjahr 2001/02 sowie die auf der Internetseite des EDÖB zugänglichen Informationen. Zur Vertiefung wurden zehn Fallstudien zu Aktivitäten des EDÖB durchgeführt; eine Zusammenfassung dieser Fallstudien liegt im Anhang 4 dieses Berichts vor. Weitere Quellen bilden die Rechtsgrundlagen, die Literatur und das rechtsvergleichende Gutachten des SIR (2010).

Hinweise zu einzelnen Datenmaterialien

Das Geschäftsverwaltungssystem des EDÖB erlaubt statistische Auswertungen anhand der aufgewendeten Zeitdauer einerseits für die verschiedenen vom DSG vorgesehenen Tätigkeiten (Beratung, Aufsicht, Information, Gesetzgebung, weitere) und andererseits für die Sachbereiche. Die Aussagekraft dieser Analysen stösst jedoch an Grenzen, da die Daten nicht für statistische Zwecke erhoben wurden. So schwankt die verbuchte Anzahl Stunden, unabhängig vom Stand der besetzten Stellen, von Jahr zu Jahr deutlich (der kleinste Wert beträgt gut 80% des grössten Werts). Die anhand dieser Daten gemachten Aussagen in diesem Bericht sollten deshalb als grobe Tendenzaussagen gelesen werden.

Zu den verschiedenen Aktivitäten des EDÖB (Beratung, Aufsicht, Information) wurden zehn Fallstudien erarbeitet, denen jeweils eine Dokumentenanalyse, Gespräche mit Mitarbeitenden des EDÖB sowie gezielte Nachfragen bei einem Teil der Datenbearbeiter zu Grunde liegen. Die nachfolgende Tabelle gibt Auskunft über die durchgeführten Fallstudien und ordnet sie den gesetzlichen Aufgabenbereichen des EDÖB zu. Die Fallstudien werden im Anhang überblicksartig dargestellt. Im Bericht selbst wird auf die jeweils interessierenden Aspekte Bezug genommen.

Fallstudie	*Aktivität*	*Bereich*	*Kurz-Bezeichnung*
SAKE: Schweizerische Arbeitskräfteerhebung des BFS	Beratung	Bundesorgan	SAKE
Baubranche	Beratung	Privat	Baubranche
AVAM: Bearbeitungsreglement Informationssystem für die Arbeitsvermittlung und die Arbeitsmarktstatistik	Sachverhaltsabklärung	Bundesorgan	AVAM
Krankenkassen-Umfrage: Erhebung über die datenschutzrechtliche Organisation bei den anerkannten sozialen Krankenversicherer	Sachverhaltsabklärung	Bundesorgane	Krankenversicherer
Google Street View	Sachverhaltsabklärung	Privat	Google Street View
Logistep (P2P-Netzwerke)	Sachverhaltsabklärung	Privat	Logistep
Mitarbeitercheck	Sachverhaltsabklärung	Privat	Mitarbeitercheck
Überwachung Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz	Information	Bundesorgane und Private	Leitfaden Überwachung
Erläuterungen zu Sozialen Netwerken	Information	Privat	Soziale Netzwerke
Erläuterungen zu Mobile Computing	Information	Privat	Mobile Computing

Die Auswahl der Fälle erfolgte in Absprache mit der Arbeitsgruppe und dem EDÖB. Sie orientiert sich neben der Verfügbarkeit der Unterlagen sowie der Berücksichtigung der verschiedenen Aktivitäten (Beratung, Aufsicht, Information) und Bereiche (Bund/Private) hauptsächlich an den Ergebnissen, die sich bei der Frage nach Herausforderungen für den Datenschutz ergeben haben (vgl. Kapitel 3 und 4).

Der Tätigkeitsbericht des EDÖB verfolgt primär den Zweck, die Öffentlichkeit zu informieren, und ist nicht ein Rechenschaftsbericht oder Geschäftsbericht im engeren Sinn. Deshalb beschreibt er die Aktivitäten des EDÖB in den verschiedenen Bereichen auch nur selektiv. Berichtet wird über jene Aktivitäten, die der EDÖB für öffentlichkeitsrelevant hält. Der Tätigkeitsbericht wurde deshalb nur ergänzend für Aussagen in diesem Bericht herangezogen. Als zusätzliche Quelle wurde dem Evaluationsteam eine Liste sämtlicher Sachverhaltsabklärungen, die im Jahr 2009/2010 abgeschlossen wurden oder noch pendent waren, zur Verfügung gestellt. Insgesamt erschwerte der Datenmangel die Beantwortung der Forschungsfragen teils erheblich.

11 Stellung und Organisation des EDÖB

In diesem Kapitel steht die Funktionsweise des EDÖB im Mittelpunkt. In einem ersten Abschnitt wird auf die institutionelle Stellung des EDÖB eingegangen, wobei hier vor allem die Frage seiner Unabhängigkeit gegenüber den Bundesorganen und den privaten Datenbearbeitern im Vordergrund steht. Der zweite Abschnitt widmet sich der Organisation des EDÖB. Auf die Organisationsstruktur der Behörde wird dabei nur kurz eingegangen. Der Schwerpunkt liegt auf der Organisation der wichtigsten Arbeitsprozesse des EDÖB, so seiner Planung und der Triage der eingehenden Anfragen und Themen. Weitere Abschnitte dieses Kapitels betreffen die Ressourcen und Zusammenarbeit und Koordination des EDÖB mit anderen Akteuren des Datenschutzes.

11.1 Stellung des EDÖB

Der Abschnitt beschreibt zunächst die aktuelle Stellung des EDÖB aus rechtlicher Sicht vor und stellt diese hernach der Stellung der Datenschutzaufsichtsbehörden in anderen Ländern gegenüber. Auch wird basierend auf Interviewaussagen und den Fallstudien der Frage seiner Unabhängigkeit in der Praxis nachgegangen.

11.1.1 Ausgangslage und Reform

Wichtige Aspekte der Unabhängigkeit einer Behörde sind die Bedingungen der Wahl, die administrative Zuordnung, die Unabhängigkeit von Weisungen sowie die Frage des Budgets und der angemessenen Ressourcen (Huber 2006: 362-378; Rosenthal/Jöhri 2008: 604-607).

Durch die Assoziierung an Schengen/Dublin ist die Schweiz verpflichtet, sich bei der Bearbeitung von Personendaten im Rahmen der Schengener und Dubliner Zusammenarbeit an die geltende Gemeinschaftsregelung zu halten. 2008 wurde die Schweiz im Hinblick auf die Inkraftsetzung des Schengen-Besitzstandes einer Evaluation durch die EU unterzogen. Letztere kam dabei unter anderem zum Schluss, die finanzielle und administrative Unabhängigkeit der nationalen Aufsichtsbehörde sei zu stärken. Der Bundesrat hat diese Forderungen, welche vom Europäischen Rat übernommen wurden, im Rahmen eines Bundesbeschlusses aufgenommen und entsprechende Anpassungen und Präzisierungen des DSG zuhanden des Parlaments verabschiedet (Bundesrat BBl 2009: 6749-6798).

Auch die Rechtslehre bemängelte die Unabhängigkeit des EDÖB im geltenden Recht ebenfalls. Sie bezog sich dabei primär auf die Wahl des Beauftragten durch den Bundesrat (Huber 2006: 366-371; Epiney 2006). Der inhaltliche Hauptgrund dafür ist die Problematik, dass der Beauftragte (Chef EDÖB) als Aufsichtsorgan der Bundesverwaltung bisher von der obersten Behörde ebendieser Bundesverwaltung gewählt worden ist (Bundesrat/BBl 2009: 6775; Rosenthal/Jöhri 2008: 604).

Die Reform wurde 2010 vom Parlament beschlossen und ist am 1. Dezember 2010 in Kraft getreten. Der revidierte Art. 26 sowie die neu eingefügten Art. 26a und 26b DSG sowie Art. 31

VDSG regeln insbesondere die Wahl, die Amtszeit und die Stellung des EDÖB präziser als bisher. Somit gilt hinsichtlich der wesentlichen Aspekte der Unabhängigkeit aktuell folgendes:

- *Wahl und Auflösung der Anstellung:* Neu wird der Beauftragte vom Bundesrat für eine Amtsdauer von jeweils vier Jahren gewählt, wobei das Parlament die Wahl zu genehmigen hat. Die Wiederwahl erfolgt automatisch, wenn der Bundesrat nicht sechs Monate vor Ablauf der Amtszeit die Nichtwiederwahl begründet verfügt. Bisher bestimmte der Bundesrat allein über die Wahl und regelte weitere Aspekte der Anstellung mit dem EDÖB. Auch die vorzeitige Auflösung des Arbeitsverhältnisses (durch beide Parteien) ist nun im DSG geregelt und an Voraussetzungen gebunden worden.[239] Eine Amtsenthebung durch den Bundesrat ist möglich, wenn der Beauftragte vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat, oder wenn er die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.

- *Anstellungsverhältnisse:* Im Übrigen richten sich die Anstellungsverhältnisse wie bisher (seit 2008) nach dem Bundespersonalgesetz (BPG). Um seine Unabhängigkeit zu stärken, wird der EDÖB jedoch explizit vom Beurteilungssystem dieses Gesetzes ausgenommen.

- *Nebenbeschäftigung:* Neu regelt das Gesetz auch die Ausübung einer Nebenbeschäftigung des Datenschutzbeauftragten. Für die Ausübung einer anderen Beschäftigung braucht der Beauftragte die Genehmigung des Bundesrates. Diese Beschäftigung darf die Unabhängigkeit und das Ansehen des Beauftragten nicht beeinträchtigen.[240]

- *Weisungsunabhängigkeit:* Die Unabhängigkeit war schon bisher explizit im Gesetz verankert. Im Rahmen der Revision ist neu konkretisiert worden, dass der EDÖB als unabhängige Behörde keine Weisungen einer Behörde erhält. Administrativ bleibt er der Bundeskanzlei angegliedert.

- *Ausstattung:* Dem EDÖB wird ein Sekretariat zugestanden, ausserdem kann er sein Personal selbst anstellen. Der EDÖB hat auch ein eigenes Budget. Dieses wird in einem besonderen Abschnitt der Bundeskanzlei ausgewiesen. Die Genehmigung des Budgets durchläuft den ordentlichen Budgetprozess. Das bedeutet, dass der Bundesrat letztlich dem Parlament auch über das Budget des EDÖB Antrag stellt. Er ist dabei nicht verpflichtet, den Eingaben des EDÖB zu entsprechen (Art. 142 ParlG).

Mit der Revision dürften die Anforderungen der EU erfüllt sein und auch die meisten Kritikpunkte der Literatur teilweise berücksichtigt worden sein; es fällt jedoch auf, dass der Bundesrat bei der Wahl trotz der Genehmigungsfunktion des Parlaments immer noch von zentraler Bedeutung ist. Dass das Gesetz weiterhin keine festgelegten subjektiven Wahlvoraussetzungen wie z.B. ein Qualifikationsprofil vorschreibt, dürfte in der Praxis zu mehr Flexibilität führen.

Mit der Regelung der Nebenbeschäftigung wird die bereits bestehende Praxis im Gesetz explizit vorgesehen. Der aktuelle Datenschutzbeauftragte Hanspeter Thür ist in einem Teilzeitpensum von 60% tätig und arbeitet nebenbei als Anwalt. Im Rahmen der Evaluation sind von den Inter-

[239] Bei einer Wahl allein durch das Parlament besteht möglicherweise das Risiko, dass politische Kriterien gegenüber fachlichen Kriterien wichtiger werden. Anders als bei Richterwahlen, wo mehrköpfige Gremien besetzt werden, ist beim Datenschutzbeauftragten die politische Ausgewogenheit schwerer sicherzustellen.

viewpartnern keine Äusserungen bezüglich allfälliger Probleme (Verfügbarkeit des Beauftragten, Unvereinbarkeiten, Interessenkonflikte) gemacht worden. Sie wurden allerdings von den Evaluatoren nicht auf dieses Thema angesprochen.

Die Befragten beim EDÖB bemängelten im Interview, dass der EDÖB vom Budgetprozess weitgehend ausgeschlossen bleibe. Man wünscht sich im Sinne einer Stärkung seiner Unabhängigkeit, Budgetanträge vor dem Bundesrat und dem Parlament selbst verfechten zu können. Wie erwähnt bilden auch die Ressourcen einen zentralen faktischen Teil der Unabhängigkeit; insofern ist dieser Wunsch nachvollziehbar. Ob eine Stärkung der Budgetunabhängigkeit des EDÖB faktisch eine Wirkung hätte – also seine Ressourcensituation beeinflussen würde – kann im Rahmen dieser Evaluation nicht abgeschätzt werden.

Dem Wunsch des EDÖB kann entgegengehalten werden, dass eine Sonderstellung im Budgetprozess bisher nur sehr wenigen Behörden eingeräumt wird: Der Bundesrat muss bisher nur die Budgets der Bundesversammlung, der eidgenössischen Gerichte, der Finanzkontrolle, der Bundesanwaltschaft und der Aufsichtsbehörde über die Bundesanwaltschaft unverändert in seinen Voranschlag zuhanden des Parlaments aufnehmen (Art. 142 Abs. 2 ParlG). Andere, bis zu einem gewissen Grad vergleichbare Aufsichtsbehörden wie etwa die Wettbewerbskommission oder der Preisüberwacher sind in der gleichen Lage wie der EDÖB. Im internationalen Vergleich ist der beschränkte Einfluss der Datenschutz-Aufsichtsbehörde auf ihr Budget kein Einzelfall. Schon heute ist überdies der Bundeskanzler verpflichtet, dem Bundesrat „alle Empfehlungen und Berichte des Beauftragten“ zu übermitteln, „selbst wenn er diesen nicht zustimmen kann“ (Art. 31 VDSG Abs. 1). Es kann davon ausgegangen werden, dass diese Bestimmung auch Stellungnahmen des EDÖB zu Budgetfragen einschliesst.

11.1.2 Wahl und Stellung im internationalen Vergleich

Im internationalen Vergleich zeigt sich bezüglich des Wahlorgans, dass in vier der neun untersuchten Länder das Parlament für die Wahl der nationalen Aufsichtsbehörde zuständig ist (vgl. Tabelle 11-1). In den übrigen Staaten übernimmt zumeist das Staatsoberhaupt diese Aufgabe (Grossbritannien, Niederlande und Österreich). Nur im Falle von Spanien findet wie in der Schweiz die Wahl durch die Regierung statt. Eine Mischform kommt in Frankreich zur Anwendung.

Die untersuchten Länder kennen durchwegs Bestimmungen zur Amtdauer: Sie beträgt in den Mitgliedstaaten der EU zwischen vier und sechs Jahren, in den kanadischen Provinzen zwischen zwei und sieben Jahren. Eine Reihe von Ländern legt zudem eine Beschränkung der Amtszeit auf maximal zwei Perioden fest (Deutschland, Frankreich, Italien, Slowenien); in Grossbritannien ist eine dritte Amtszeit nur unter bestimmten Bedingungen möglich.

In mehreren Ländern finden sich Bestimmungen zu den Wahlvoraussetzungen: In Deutschland müssen Kandidaten das 35. Lebensjahr vollendet haben und die Befähigung zur Bekleidung öffentlicher Ämter besitzen. Die Mitglieder der österreichischen Datenschutzkommission müssen

[240] In Deutschland wird eine solche Nebenbeschäftigung explizit ausgeschlossen (SIR 2010: 68).

rechtskundig sein; auch in Italien werden fachliche Anforderungen an die Kandidaten gestellt. In Slowenien dürfen (nebst dem Vorhandensein eines Universitätsabschlusses und fünfjähriger Arbeitserfahrung) keine Vorstrafen bestehen. Ebenfalls äussert sich die Rechtsordnung in einzelnen Ländern zur Immunität (z.B. Kanada), den Auflösungsgründen (z.B. Slowenien) oder zur Unvereinbarkeit mit anderen Tätigkeiten (z.B. Italien).

Beträchtliche Unterschiede lassen sich bezüglich der organisatorischen Ausgestaltung der Datenschutzbehörde feststellen. Vier der neun untersuchten Länder verfügen über eine Kollegialbehörde, die übrigen Länder kennen wie die Schweiz ein hierarchisches System (ausführlicher vgl. Ziffer 11.2.1). Administrativ sind die Aufsichtsbehörden bei einem Teil der Länder (Deutschland, Grossbritannien, Niederlande, teilweise Kanada) bestimmten Ministerien zugeordnet. In Frankreich, Spanien und Italien sind die Aufsichtsbehörden stärker von der Verwaltungsorganisation losgelöst. Die Regelung, dass die Aufsichtsbehörde weisungsunabhängig handeln kann, ist weit verbreitet.

Beim Budget findet sich in den untersuchten Staaten kein einheitliches Modell; in der Regel hat das Parlament das letzte Wort. Die Aufsichtsbehörden einiger Länder kennen im Gegensatz zur schweizerischen Situation teilweise die Möglichkeit, ihr Budget selber beantragen und verteidigen zu können (z.B. Spanien, Slowenien).

Tabelle 11-1: Wahl und Stellung im internationalen Vergleich

	Wahlorgan	*Amtsdauer*	*Organisation*	*administrative Zuordnung*
DE	Parlament	5 Jahre, Wiederwahl einmalig möglich	hierarchisch	Bundesministerium des Inneren
F	Mischform	5 Jahre, Wiederwahl einmalig möglich	kollegial	unabhängige Behörde
GB	Staatsoberhaupt	5 Jahre, Wiederwahl einmalig möglich*	hierarchisch	Justizministerium
NL	Staatsoberhaupt	6 Jahre, Wiederwahl möglich	kollegial	Justizministerium
IT	Parlament	4 Jahre, Wiederwahl einmalig möglich	kollegial	unabhängige Behörde
CND	Parlament	2-7 Jahre, je nach Staat	hierarchisch	z.T. Parlament, z.T. Ministerium
ÖS	Staatsoberhaupt	5 Jahre, Wiederwahl möglich	kollegial	keine Angabe
SL	Parlament	5 Jahre, Wiederwahl einmalig möglich	hierarchisch	keine Angabe
ES	Regierung	4 Jahre	Aufsichtsbehörde: hierarchisch; Konsultativrat: kollegial	unabhängige Behörden
CH	*Regierung, Genehmigung durch Parlament*	*4 Jahre, Wiederwahl einmalig möglich*	*hierarchisch*	*Bundeskanzlei*

Angaben (ausser CH) basierend auf SIR (2010).

Mit der Revision des DSG, die auf den 1. Dezember 2010 in Kraft getreten ist, hat sich die Schweiz den übrigen Ländern angenähert, insbesondere was die Festlegung der Amtsdauer und die Regelung der Wiederwahl betrifft (allerdings nicht bezüglich der Beschränkung der Amtsdauer insgesamt). Auch die Möglichkeit der Amtsenthebung ist neu gegeben. Die Tatsache, dass der EDÖB sein Budget nicht selber verteidigen kann und nicht durch das Parlament (allein) gewählt wird, stellt im internationalen Vergleich keinen Sonderfall dar. Die Wahl durch die Regierung kennt neben der Schweiz jedoch nur Spanien. In Grossbritannien, Österreich und den Niederlanden liegt die Wahlkompetenz beim Staatsoberhaupt.

11.1.3 Erfahrungen aus der Praxis

Die beschriebene Reform des DSG bezüglich seiner Wahl und Stellung orientiert sich an der oben zusammengefassten rechtlichen Diskussion, die zudem stark auf die Unabhängigkeit des EDÖB gegenüber den Bundesbehörden fokussiert ist. Empirische Erkenntnisse zur Frage, inwieweit der EDÖB in der Praxis unabhängig agiert und auch gegenüber Einflussversuchen von privaten Datenbearbeitern resistent ist, fehlen bislang. Ein definitives Urteil ist auch im Rahmen dieser Evaluation nicht möglich. Die Interviews mit den Experten und Bearbeitern erlauben jedoch gewisse Schlussfolgerungen.

Die im Rahmen dieser Evaluation durchgeführten Interviews bei den Bearbeitern, Experten und Interessengruppen erbrachten keine Hinweise darauf, dass sich die aus rechtlicher Sicht insbesondere bis November 2010 mangelhafte Unabhängigkeit auf die Praxis des EDÖB negativ ausgewirkt hätte, oder dass seine Unabhängigkeit in Zweifel gezogen worden wäre. Beide Interessenvertreter und auch die Technologieexperten (soweit sie sich darüber ein Urteil zutrauen) beurteilen die Unabhängigkeit des EDÖB gegenüber den Behörden und den privaten Bearbeitern in der Praxis als gegeben. Dieser Einschätzung schliessen sich auch die Rechtsexperten weitgehend an. Ein Experte bezeichnet die Unabhängigkeit als theoretisch gegeben, kommt aber gleichzeitig zum Schluss, dass der Grad der Unabhängigkeit auch stark von der Person abhänge, welche das Amt ausübe. Er verneint, dass aktuell diesbezüglich ein Problem bestehe. Mit den beschlossenen Amtsenthebungsgründen ist hier im Übrigen neu eine Sicherung gegenüber Fehlbesetzungen im Gesetz eingebaut worden.

Auch die Interviewaussagen der Bearbeiter zum EDÖB deuten nicht darauf hin, dass diese ihn als abhängig wahrnehmen. Allerdings haben Bearbeiter auch kaum ein Interesse, den EDÖB als abhängig darzustellen. In der Tendenz wurde der Chef EDÖB (und sein Team) von den Bearbeitern recht wohlwollend als kompetent und überwiegend als realitätsnah beschrieben, was einzelne Konflikte aber nicht ausschliesse. Mehrere (private) Bearbeiter gaben an, sich gut zu überlegen, mit welchen Fragen und Problemstellungen sie sich an den EDÖB wenden, um nicht „schlafende Hunde zu wecken“. Dies deutet darauf hin, dass der EDÖB als Verfechter des Datenschutzes ernst genommen wird, was als Hinweis auf seine Unabhängigkeit gelesen werden kann.

Laut den Interviewpartnern beim EDÖB ist die Unabhängigkeit des EDÖB gegeben. Sie sei nicht etwas, das einfach bestehe. In der materiellen Arbeit sei die Unabhängigkeit gewährleistet. Doch man müsse andere Behörden immer wieder an die Stellung des EDÖB erinnern, wenn man z.B. Informationsbedürfnisse habe und diese auch durchsetzen wolle. Ein Mangel an Unab-

hängigkeit bestehe am ehesten im Budgetbereich, wo man nicht die volle Kontrolle über die Mittel habe. Aber dies sei keine Bremse in der täglichen Arbeit. Seitens der Bundesbehörden hat der EDÖB keine offenen Druckversuche festgestellt. Man erhalte die Informationen, die man benötige, auch wenn man gelegentlich nachhaken müsse. Das hänge aber nicht mit der Frage der Unabhängigkeit zusammen. Seitens von Privaten sei es auch schon vorgekommen, dass diese sich bei anderen Behörden beschwert hätten. Aber solche Beschwerden seien vollkommen wirkungslos, die kontaktierten Behörden leiteten diesen Druck nicht weiter.

In den durchgeführten Fallstudien schliesslich haben sich keine Hinweise für eine mangelnde Unabhängigkeit des EDÖB ergeben. Gerade bei den Sachverhaltsabklärungen im Privatbereich hat sich gezeigt, dass der Datenschutzbeauftragte bereit ist, die ihm zur Verfügung stehenden rechtlichen Möglichkeiten (vorsorgliche Massnahme, Empfehlung, Rechtsweg) auszuschöpfen, woraus sich zumindest in diesen Fällen auf eine ausreichende Unabhängigkeit schliessen lässt.

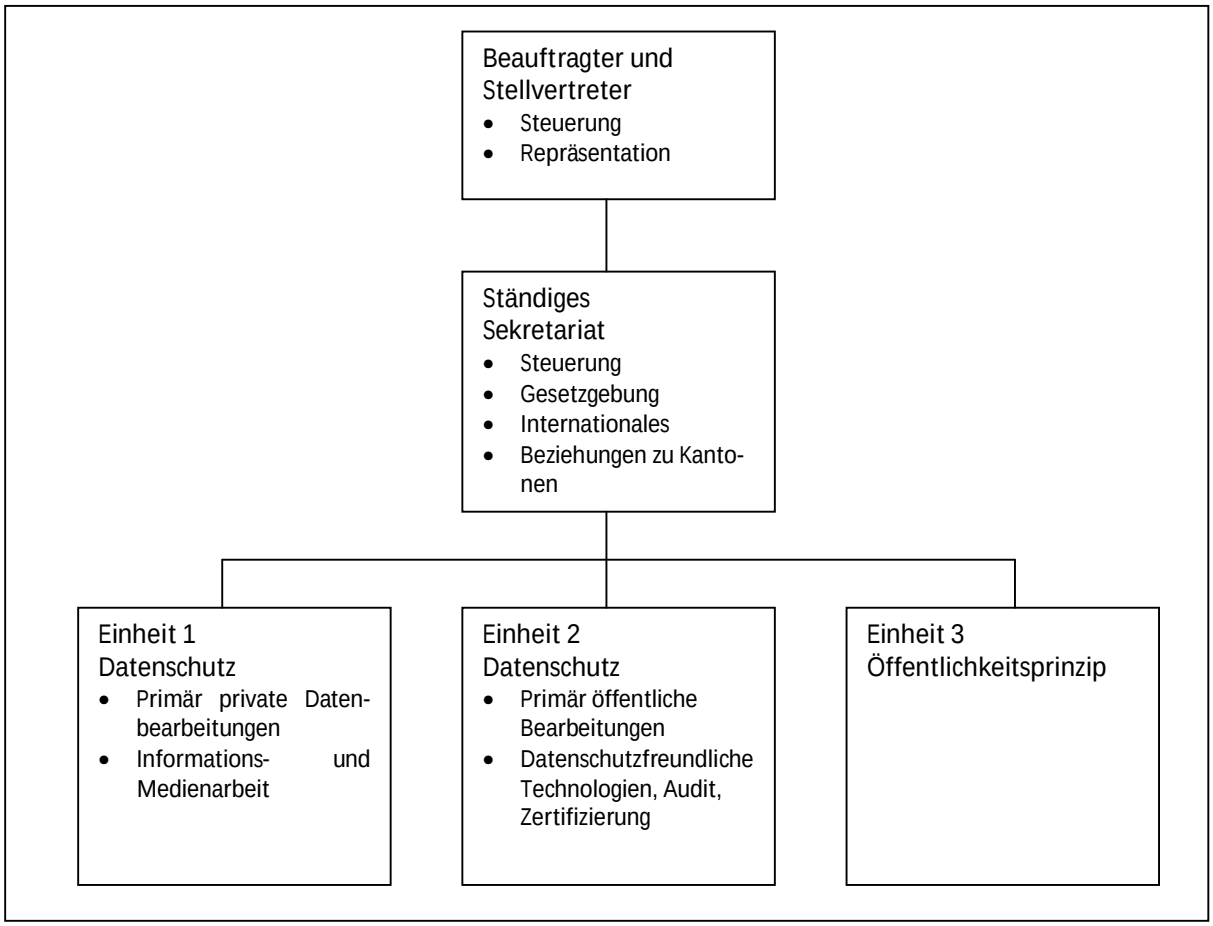
11.2 Organisation und Steuerung der Aktivitäten des EDÖB

Dieser Abschnitt beschäftigt sich mit der Steuerung der Aktivitäten und mit den wichtigsten Prozessen des EDÖB. Zunächst ist kurz die Struktur der Aufsichtsbehörde zu beschreiben. Danach wird auf die wichtigsten Steuerungsprozesse eingegangen. Ebenfalls sollen an dieser Stelle die Ressourcensituation beim EDÖB und die Auswirkungen der Doppelfunktion als Datenschutz- und Öffentlichkeitbeauftragter diskutiert werden.

11.2.1 Organisation der Struktur inklusive internationaler Vergleich

Die Organisationsstruktur des EDÖB ist in leicht vereinfachter Form in Abbildung 11-1 wiedergegeben. Als Kopf der Organisation amten die Person des Beauftragten (aktuell Hanspeter Thür) und sein Stellvertreter. Das ständige Sekretariat besteht aus dem stellvertretenden Beauftragten und einem Stellvertreter. Die operativen Tätigkeiten werden in drei Einheiten ausgeübt, wovon eine für die Durchsetzung des Öffentlichkeitsprinzips nach BGÖ zuständig ist und deren zwei für die Umsetzung des DSG. Einheit 1 ist primär für den Datenschutz im privaten Sektor zuständig. Dieser wird in sechs Teilbereiche untergliedert. Der Chef dieser Einheit ist zusätzlich verantwortlich für die Informationstätigkeit (Internetauftritt) und die Medienarbeit, wobei gegen Aussen oft der Beauftragte selbst als „Gesicht“ seiner Behörde auftritt. Einheit 2 ist primär für Datenbearbeitungen der Bundesorgane zuständig. Der Chef dieser Einheit betreut zusätzlich die Bereiche datenschutzfreundliche Technologien, Datenschutz-Audits und Zertifizierungen nach Art. 11 DSG.

Abbildung 11-1: Organigramm des EDÖB



Quelle: http://www.edoeb.admin.ch. Vereinfachte Darstellung.

Im internationalen Vergleich zeigen sich hinsichtlich der Organisationsstruktur zwei Modelle (vgl. Tabelle 11.1). Ähnlich wie die Schweiz kennen Deutschland, Grossbritannien, Kanada, Slowenien und Spanien hierarchische Organisationsformen mit einem Datenschutzbeauftragten (oder analogen Bezeichnungen) an der Spitze. In Spanien besteht daneben zusätzlich ein Konsultativrat. In Frankreich, Italien, Österreich und Holland ist hingegen eine Kollegialbehörde zuständig. Ersichtlich ist in diesen Ländern insbesondere das Bemühen, einerseits Expertise aus den relevanten Bereichen (Informatik und Recht) und andererseits die verschiedenen Interessen in der obersten Datenschutzbehörde zu versammeln (SIR 2010).

In Frankreich besteht die „Commission Nationale de l'Informatique et des Libertés (CNIL)", aus 17 Mitgliedern, die aus verschiedenen Kompetenzbereichen rekrutiert werden (Parlament, Wirtschafts-, Sozial- und Umweltrat[241], Gerichte, Experten).

In Italien ist der „Garante per la protezione dei dati personali" eine Kommission aus vier Mitgliedern mit dem Status einer „Autorità Amministrativa Indipendente".

[241] Dabei handelt es sich um ein Konsultativorgan des Parlaments und der Regierung.

In Österreich besteht die Datenschutzkommission als unabhängige Kollegialbehörde und gerichtsähnliche Organisation aus sechs rechtskundigen, nebenamtlichen Mitgliedern inklusive eines geschäftsführenden Mitglieds. Das vorsitzende Mitglied muss dem Richterstand angehören. Die Regierung muss bei ihrem Wahlvorschlag zuhanden des Bundespräsidenten Vorschläge folgender Kreise berücksichtigen: Richterstand, Länder, Bundeskammer für Arbeiter und Angestellte, Wirtschaftskammer, Bundesbedienstete. Der Bundeskanzler muss der Kommission eine Geschäftsstelle einrichten. Neben der Kommission existiert ein Datenschutzrat, dem beratende Funktion in rechtspolitischen Fragen des Datenschutzes zukommt.

In Spanien besteht die „Agencia de Protección de Datos" aus einem Direktor und einem Konsultativrat („Consejo Consultivo"). Der Präsident wird von der Regierung aus dem Kreis des Konsultativrats gewählt. Der Konsultativrat rekrutiert sich aus folgenden Kreisen: Parlament, Verwaltung, Autonome Gemeinschaften, Gemeinden und Provinzen, Königliche Akademie für Geschichte, Universitätsrat, Konsumentenrat, Rat der Handels-, Industrie- und Schifffahrtskammern.

In Holland besteht die Datenschutzbehörde aus einem Vorsitzenden und zwei weiteren Mitgliedern. Zusätzlich können spezielle Mitglieder ernannt werden, welche die verschiedenen Sektoren der Gesellschaft repräsentieren sollten. Letzteres gilt auch für den 14köpfigen Rat, der der Datenschutzbehörde in generellen Fragen beratend zur Seite steht.

11.2.2 Schwerpunktsetzung – begrenzte Steuerbarkeit der Aktivitäten

Die Planbarkeit der Aktivitäten des EDÖB ist beschränkt, da diese sich stark nach den Bedürfnissen der Betroffenen und der Datenbearbeiter zu richten haben. Fragen, Beschwerden und Hinweise aus der Bevölkerung, von Bearbeitern, aber auch Hinweise in den Medien sind die wichtigsten Auslöser von Aktivitäten in den verschiedenen Bereichen. Auch die Gesetzgebungsprojekte, zu denen der EDÖB Stellung nimmt, bilden einen nicht steuerbaren Input, auf den der EDÖB zu reagieren hat. Im Einzelfall ist es oft schwer abzuschätzen, welchen Aufwand ein einzelner Fall verursacht. So hängt der Aufwand bei Sachverhaltsabklärungen stark davon ab, ob der Bearbeiter gewillt ist, eine allfällige Verbesserungsmassnahme oder Empfehlung umzusetzen, oder ob es zu einer gerichtlichen Auseinandersetzung kommt. Weitere Quellen von Aktivitäten bilden der Austausch mit anderen Datenschutzbehörden und das Register der Datensammlungen, wobei neu angemeldete Sammlungen zum Auslöser für Nachfragen oder allfällige Kontrollen werden können.

Die Vielfalt an auslösenden Momenten, die sich nur schon in den Fallstudien findet, untermauert die Aussagen der Interviewpartner beim EDÖB, wonach dessen Agenda durch Themen bestimmt wird, die auf verschiedensten Kanälen an ihn herangetragen werden. So sind es z.B. nicht nur Betroffene, sondern auch Bearbeiter, die bisweilen Interesse an Informationen anmelden. Einen Sonderfall stellt der Fall *Logistep* dar, da hier der Hinweis von ausländischen Datenschutzbehörden kam. Ebenfalls eine besondere Konstellation bilden die Kontrollen von Bearbeitungsreglementen (Fallstudie *AVAM)*. Hierzu wählt der EDÖB anhand des Registers der Datensammlungen jährlich rund zehn Fälle aus, die er sichtet. Eine kleinere Auswahl davon wird vertieft analysiert.

Tabelle 11-2: Fallstudien: Auslösende Momente von Aktivitäten des EDÖB

Fall	*Auslösendes Moment*	*Aktivität*
Google Street View	Ankündigung und Durchführung in anderen Ländern, grosse Medienaufmerksamkeit. Prüfung bei Aufschaltung des Dienstes.	Aufsicht
Logistep	Hinweise von ausländischen Datenschutzbehörden	Aufsicht
Mitarbeiter-Check	Werbemails des Anbieters. Diese führen zu mehreren Anfragen an den EDÖB	Aufsicht
AVAM	Kontrolle eines Bearbeitungsreglements eines Bundesorgans; wird ausgelöst durch Auswahl im Register der Datensammlungen. Jährliche Stichprobe umfasst auch dieses Reglement	Aufsicht
Umfrage Krankenversicherung	Mängel bei einer einzelnen Krankenkasse lösen das Bedürfnis nach einer umfassenden Umfrage aus. Zusammenarbeit mit dem BAG für Durchführung existenziell	Aufsicht
Soziale Netzwerke	Anfragen von Betroffenen und Drittpersonen (Eltern); grosses Medieninteresse am Thema, erwachendes Interesse der Politik	Information
Mobile Computing	Anfragen von Kleinunternehmen mit mangelndem technischem Know-how; Thema in Fachzeitschriften	Information
Leitfaden Überwachung am Arbeitsplatz	Regelmässige Anfragen von betroffenen Arbeitnehmern, aber auch Arbeitgebern und Organisationen; diverse Sachverhaltsabklärungen deuten auf allgemeinen Informationsbedarf	Information
SAKE	Beschwerden von Betroffenen der Umfrage, Hinweis eines kantonalen Datenschutzbeauftragten	Beratung
Baubranche	Privater Bearbeiter wendet sich an kantonalen Datenschutzbeauftragten, welcher die Anfrage weiterleitet.	Beratung

Trotz dieser stark inputorientierten Arbeitsweise versucht der EDÖB, seine Aktivitäten zu planen. Basierend auf der Auswertung der eingehenden Anfragen sowie seiner Beobachtung der Entwicklung in den Medien, der Politik, der Fachliteratur und der technologischen Entwicklung, versucht der EDÖB frühzeitig, sich abzeichnende Themen und Trends zu erkennen, um für sich Schwerpunktgebiete abzuleiten und um auf auftauchende Themen vorbereitet zu sein. So seien zum Beispiel Fragen im Zusammenhang mit der Volkszählung 2010, mit der Einführung des biometrischen Passes oder der Fussball-Europameisterschaft (Ticketing, Hooligan-Datenbank) früh absehbar gewesen, und der EDÖB sei diesen Ereignissen gut vorbereitet begegnet.

Die Festlegung solcher strategischen Schwerpunkte und die vorgenommene Gewichtung der verschiedenen Aktivitäten erfolgt gemäss den Interviewaussagen im Jahresturnus. Innerhalb der einzelnen Einheiten wird hernach konkreter festgelegt, in welchen Sachbereichen die Akzente gesetzt werden sollen. Diese Ziele werden immer im September für das folgende Jahr festgelegt und bilden die Richtschnur für die Triage der eingehenden Anfragen im Einzelfall. Nach Aussagen der interviewten Mitarbeiter strebt der EDÖB an, rund 40 bis 50% seiner Tätigkeiten im Voraus zu planen, der Rest ist reaktiv. Angesichts der begrenzten Planbarkeit seien jedoch während des Jahres häufig Zielkorrekturen notwendig. Hiermit wird beim EDÖB teilweise auch erklärt, weshalb dieser seine Ziele nicht vorab publiziert. Der Hauptgrund dafür sei allerdings, dass

insbesondere Abklärungen Diskretion benötigten und eine Vorankündigung der Schwerpunktbereiche kontraproduktiv sei.

11.2.3 Fall-Triage und -Priorisierung als zentraler Steuerungsprozess

Im Rahmen einer internen Reform hat der EDÖB für die Steuerung seiner Aktivitäten im Einzelfall einen Triage-Prozess definiert, den jede eingehende Anfrage durchläuft. Anhand von klar bestimmbaren und aus dem Gesetz abgeleiteten Kriterien soll dabei entschieden werden, ob und mit welcher Dringlichkeit ein bestimmtes Geschäft zu bearbeiten ist. In diese Triage fallen auch Geschäfte, die der EDÖB gemäss dem BGÖ zu bearbeiten hat. Sie werden in der folgenden Beschreibung aber nicht weiter beachtet. Nachfolgend wird dieser Prozess dargestellt. Festgehalten sei, dass im Rahmen der Evaluation nicht systematisch überprüft wurde, ob der Prozess in der alltäglichen Praxis tatsächlich konsequent eingehalten wird.

Der EDÖB ordnet jede eingehende Anfrage einer von vier Kategorien A bis D zu. Der Entscheid über die Zuordnung zur zuständigen Einheit fällt durch die Direktion (Einheitschefs und stellvertretender Beauftragter im Dialog mit der zuständigen Sachbearbeiterin/dem zuständigen Sachbearbeiter). Nötigenfalls kann auch der Beauftragte hinzugezogen werden. Die Bearbeitung erfolgt nachher innerhalb der Einheit.

- *Kategorie A – Bearbeitung:* Hierunter fallen alle Geschäfte, die zwingend sofort bearbeitet werden müssen. Dies kann erstens der Fall sein, weil eine Vorschrift des DSG dies explizit verlangt. Zur dieser Gruppe von Geschäften sind insbesondere folgende zu zählen: Anmeldungen von Datenbanken im Register, indirekte Auskunft, Information über Datenbekanntgaben ins Ausland, Stellungnahmen zu Gesetzgebungsvorhaben des Bundes, Kontrollen im Rahmen von Schengen/Dublin, Pilotversuche nach Art. 17a DSG. Auch Medienanfragen werden dieser Kategorie zugeordnet. Zweitens fallen Geschäfte in Kategorie A, die aufgrund ihrer Bedeutung nach einer genaueren Abklärung verlangen. Die Kriterien, nach denen Zuordnung erfolgt, werden nachfolgend beschrieben.

- *Kategorie B – Bearbeitung nach Ressourcen:* Hierunter fallen Geschäfte, die zwar grundsätzlich als wichtig erachtet werden, die aber nur bei ausreichenden Ressourcen bearbeitet werden.

- *Kategorie C – Beobachtung:* In diese Kategorie fallen Geschäfte und dabei insbesondere Anfragen und Hinweise von Betroffenen, die zwar auf ein reales Problem verweisen, als Einzelfall jedoch keine oder noch keine vertiefte Abklärung rechtfertigen. Sie werden einerseits beantwortet[242], andererseits aber auch gesammelt und nach einer Frist von einem bis drei Monaten erneut gesichtet. Zeigt es sich, dass sich Anfragen vom selben Typ mehren (z.B. Klagen von mehreren Betroffenen über denselben Bearbeiter oder denselben Typ einer Bearbeitung), so kann dies für den EDÖB zum Anlass für eine vertiefte Auseinandersetzung mit dem Thema werden, also eine Bearbeitung im Sinne von Typ A oder B. Wenn nicht, wird der Fall in Kategorie D verwiesen. Beispiele, in denen eine Anhäufung von Einzelanfragen

[242] Näheres zum Umgang mit Anfragen von Betroffenen vgl. Ziffer 12.2.4.

schliesslich zu einer Sachverhaltsabklärung führten, sind die Einführung der Kundenkarten „Cumulus“ und „Supercard“ bei Migros und Coop (vgl. EDSB 2005/2006). Die Kategorie C trägt nach Auskunft der Interviewpartner beim EDÖB nicht nur zum Erkennen relevanter Trends von Datenschutzproblemen bei, sondern auch dazu, dass die anfragenden Betroffenen oder Bearbeiter mittels Schreiben korrekt über die Vorgehensweise des EDÖB informiert werden.

- *Kategorie D – Archivierung:* Alle übrigen Anfragen werden klassiert und abgelegt, aber nicht weiter bearbeitet.

Wenn nicht eine spezifische DSG-Bestimmung die Bearbeitung und damit die Zuweisung in Kategorie A vorschreibt, ergibt sich die Zuordnung aufgrund der Relevanz des konkreten Falles und der Tätigkeitsschwerpunkte, die der EDÖB sich im Rahmen der Jahresplanung selbst vorgibt. Die Kriterien für die Zuordnung der Fälle zu den vier Kategorien sind aus dem Datenschutzgesetz abgeleitet, doch lässt der EDÖB auch zusätzliche Elemente einfliessen. Die in Frage stehende Bearbeitung muss verschiedene Eigenschaften aufweisen, damit sie Gegenstand einer Sachverhaltsabklärung oder einer anderen Aktivität wird. Die primären Kriterien sind dabei:

- *Eigenschaft der Daten:* Eine Bearbeitung ist wahrscheinlicher, wenn besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden oder wenn das Risiko einer schweren Verletzung der Persönlichkeitsrechte besteht.
- *Zahl der Betroffenen:* Die Bearbeitung wird wahrscheinlicher, je mehr Personen betroffen sind.
- *Kombination dieser Kriterien:* Diese Kriterien werden bei der Abwägung kombiniert: Je grösser die Zahl der Betroffenen, desto eher wird der EDÖB auch bei vergleichsweise wenig sensiblen Daten aktiv; je sensibler die Daten, desto eher wird der EDÖB auch bei vergleichsweise wenigen Betroffenen aktiv.

Bei der Abwägung über die Durchführung einer Aktivität spielen neben diesen Kriterien, die sich unmittelbar auf die Eigenschaften des Falls beziehen, weitere Indikatoren eine Rolle:

- *Vertrauenswürdigkeit der Quelle:* Informationen von Insidern (z.B. einem Personalchef) erhalten ein höheres Gewicht als Informationen von Outsidern.
- *Subordinationsverhältnis:* Wenn sich die betroffenen Personen in einem Subordinationsverhältnis zum Bearbeiter befinden (z.B. als Arbeitnehmer), sieht sich der EDÖB eher zu einer Sachverhaltsabklärung veranlasst.
- *Präzedenzfall:* Eine wichtige Rolle spielt die Frage, ob der konkrete Fall exemplarisch für andere Fälle steht, also einen Präzedenzfall darstellt. So kann zum Beispiel die Sachverhaltsabklärung zur Videoüberwachung bei einer Aldi-Filiale durchaus als Musterfall für den gesamten Detailhandel betrachtet werden (vgl. EDÖB 2006/07).
- *Klärung der Rechtslage:* Wenn ein Sachverhalt sich potenziell eignet, noch offene Rechtsfragen zu klären oder die gesetzlichen Datenschutzgrundsätze zu konkretisieren, wird eine Sachverhaltsabklärung ebenfalls wahrscheinlicher. So konnte mit einer Sachverhaltsabklä-

rung im Internetbereich geklärt werden, dass IP-Adressen bis zu einem gewissen Grad als Personendaten betrachtet werden können (vgl. Fallstudie *Logistep*). Bei *Google Street View* soll nicht zuletzt die Frage beantwortet werden, ob Individuen damit zu rechnen haben, dass sie auf Internet sichtbar sein können, sobald sie ihren Privatraum verlassen haben.

In die Entscheidung, ob eine Sachverhaltsabklärung durchgeführt wird (und wie der EDÖB darüber kommuniziert), fliessen schliesslich bei grösseren Fällen Überlegungen zum politischen, medialen und internationalen Umfeld ein. Medialer Druck oder eine aufkommende politische oder internationale Debatte können dazu führen, dass eine Fragestellung höhere Priorität erhält.

11.2.4 Weitere Prozesse

Für die Durchführung der verschiedenen Aktivitäten des EDÖB bestehen in der Behörde klare Ablaufschemata, welche die einzelnen Arbeitsschritte und die Zuständigkeiten für die Bearbeitung und die jeweils zu fällenden Entscheidungen definieren. Am weitesten ausgebaut sind die Arbeitsgrundlagen bei der Sachverhaltsabklärung, da hier der EDÖB potenziell am stärksten in die Sphäre der Bearbeiter eingreift und seine möglichen Empfehlungen gerichtsfest sein müssen. Ablaufschemata, welche die Zuständigkeiten und Verwantwortlichkeiten regeln, bestehen für folgende Prozesse:

- Umgang mit Posteingängen
- Umgang mit telefonischen Anfragen
- Stellungnahmen zu Gesetzgebungsvorhaben
- Erstellung von Erläuterungen auf der Website
- Erstellung von Leitfäden oder Merkblättern
- Website-Publikation
- Veranstaltungen (Vorträge, Konferenzen, Kurse)
- Durchführung von Sachverhaltsabklärungen inkl. Nachkontrolle

11.2.5 Doppelfunktion für DSG und BGÖ

Seit Inkrafttreten des Öffentlichkeitsgesetzes im Jahr 2006 ist der Datenschutzbeauftragte für die Umsetzung sowohl des DSG als auch des BGÖ zuständig. Vor- und Nachteile dieser Doppelfunktion für den Vollzug des DSG wurden in den Interviews mit den Experten angesprochen. Ferner stützen sich die nachfolgenden Ausführungen auf die bereits bestehende Evaluation des BGÖ.

In der Botschaft des Bundesrates zum Öffentlichkeitsgesetz (Bundesrat 2003: 2029) wurde die Übertragung der Aufgaben im Rahmen des BGÖ an den damaligen EDSB folgendermassen begründet: Zwar würden sich die Aufgabenbereiche von Datenschutz- und Öffentlichkeitsbeauftragten unterscheiden; es sei indessen absehbar, dass sich im Verfahren betreffend Zugang zu

amtlichen Dokumenten, welche Personendaten enthalten, oft datenschutzrechtliche Fragen stellen würden. Daher sei es sinnvoll, den Datenschutzbeauftragten mit der Wahrnehmung der Schlichtungs- und Beratungsaufgaben nach Öffentlichkeitsgesetz zu beauftragen, damit das Zugangsverfahren möglichst einfach bleibe und Synergien genutzt werden könnten. Zudem könne damit auch den von einigen Vernehmlassern geäusserten Bedenken Rechnung getragen werden, dass mit der Einführung des Öffentlichkeitsprinzips der Schutz von Personendaten beeinträchtigt werden könnte.

Die Interviewpartner sehen vor allem zwei Vorteile in der Doppelfunktion. Positiv beurteilt wird, dass eine Koordination zwischen den beiden Bereichen stattfinde und damit gemäss einem Rechtsexperten unter Umständen auch verhindert werden kann, dass eines der beiden Prinzipien als absolut behandelt werde. Ebenfalls als Vorteil wurde erwähnt, dass beide Tätigkeiten Unabhängigkeit gegenüber der Regierung und der Verwaltung erfordern. Dies sei mit der heutigen Situation gegeben. Drei Interviewpartner beurteilen die Doppelfunktion nicht als grundsätzliches Problem.

Ein Nachteil wird darin gesehen, dass die beiden Bereiche nach unterschiedlichen Grundsätzen funktionieren und es somit heikel sei, wenn sie von derselben Stelle ausgeübt würden. Ein Interessenvertreter bezeichnete dies als Problem. Daneben gelte es insbesondere zu berücksichtigen, dass durch die Aufgaben im Rahmen des BGÖ zusätzliche Ressourcen gebunden würden, die nicht entsprechend kompensiert worden seien. Tatsächlich ging der Bundesrat in seiner Botschaft zum BGÖ davon aus, dass dem Öffentlichkeitsbeauftragten 3,5 Stellen zusätzlich zur Verfügung stehen sollten. Diese wurden aber nach Inkraftsetzung des BGÖ dem EDÖB nicht bewilligt.

Ergänzend kann das Register der Datensammlungen erwähnt werden, das die Überschneidung der beiden Bereiche veranschaulicht. Es hat zwar primär die Funktion des Datenschutzes, indem es die Bürgerinnen und Bürger über bestehende mögliche Bearbeitungen seiner persönlichen Daten aufklären soll. Da Bundesbehörden jede Sammlung anmelden müssen, dient das Register aber auch der Transparenz.

Zu ähnlichen Befunden, aber zu einer anderen Wertung kommt die Studie zur Evaluation des Öffentlichkeitsgesetzes (IDHEAP 2009: 22; 40). Die Zuweisung von Aufgaben des DSG und des BGÖ an den EDÖB führe zu Problemen: Zwar liessen sich bestimmte Tätigkeiten leichter von einer Instanz beurteilen, welche gleichzeitig für den Datenschutz und das Öffentlichkeitsprinzip zuständig sei. Gemäss dem Bericht bezeichnen verschiedene befragte Experten jedoch die „Aufgabenkonzentration als ambivalent, denn die zum Teil widersprüchlichen Rollen zeugen von unterschiedlichen Kulturen: Die eine begünstigt die Öffnung, die andere den Schutz der Information. Die Funktion des Öffentlichkeitsbeauftragten sollte in jedem Fall über von der Funktion des Datenschutzbeauftragten unabhängige spezifische Ressourcen verfügen“ (IDHEAP 2009: 40). Der EDÖB entscheidet heute autonom darüber, welchen Anteil seiner Personalressourcen er für die Aufgaben im Bereich des BGÖ einsetzt. Anfang 2010 waren es nach Auskunft des EDÖB 1.6 Stellen.

11.2.6 Dokumentation und Nachvollziehbarkeit der Planung und Umsetzung

Wie oben ausgeführt wurde, verfügt der EDÖB im Bereich der Steuerung seiner Aktivitäten über klar definierte Prozesse und Entscheidungskriterien. Dies betrifft insbesondere die Bearbeitung und Triage der eingehenden Anfragen. Trotz der begrenzten Planbarkeit der Geschäfte versucht der EDÖB im Rahmen von Jahresplanungen Schwerpunktthemen festzulegen, wobei er seinen Angaben zufolge den Ressourceneinsatz häufig kurzfristig anpassen muss. Kritisch anzumerken bleibt, dass der EDÖB über seine Schwerpunktsetzung und die tatsächliche Umsetzung zumindest gegen aussen keine Transparenz schafft.

Ein ähnlicher Mangel besteht auch ganz allgemein hinsichtlich der Dokumentation der Aktivitäten des EDÖB. Als zentrale Informationsquellen hierfür bestehen einerseits das Geschäftsverwaltungssystem des EDÖB, das eine ungefähre Gliederung des Zeitaufwands nach Aktivitäten und nach Sachbereichen erlaubt, sowie der Tätigkeitsbericht. Letzterer versteht sich jedoch nicht primär als Rechenschaftsbericht, in welchem der EDÖB über das Erreichte im vergangenen Jahr umfassend und im Sinne einer Zielerreichungskontrolle Bilanz zieht. Er dient primär der Darstellung von Fällen, in denen der EDÖB im jeweils vergangenen Jahr aktiv war und denen der EDÖB eine besondere öffentliche Bedeutung zuschreibt. Diese Funktion des Tätigkeitsberichts ist zwar sinnvoll, jedoch nicht die einzig Vorstellbare. So stehen heute beispielsweise folgende steuerungsrelevante Informationen weder dem EDÖB noch der Öffentlichkeit zur Verfügung:

- Anzahl durchgeführter Sachverhaltsabklärungen und Prozentsatz der Sachverhaltsabklärungen, die zu Empfehlungen führen. Dies verhindert auch die Ermittlung einer präzisen Erfolgsbilanz. Aufschlüsselung dieser Abklärungen nach privaten und öffentlichen Datenbearbeitern.
- Anzahl Stellungnahmen in Rechtsetzungsprozessen und Durchsetzungsquote dieser Stellungnahmen.
- Zeitaufwand des EDÖB für die Beratung von Betroffenen im Vergleich zu Bearbeitern.
- Zeitaufwand des EDÖB für Datenbearbeitungen von Bundesorganen im Vergleich zu privaten Datenbearbeitern.

Infolgedessen zieht der EDÖB weder in seinem Tätigkeitsbericht noch anderswo Bilanz über seine Aktivitäten und Erfolge und Misserfolge. Auch enthält der Tätigkeitsbericht keine Zusammenfassung der Gesamtentwicklung aus datenschutzrechtlicher Perspektive, was von der höchsten Datenschutzbehörde des Bundes jedoch durchaus erwartet werden kann. Solche Stellungnahmen nimmt der EDÖB höchstens fragmentarisch im Rahmen von Vorträgen vor, die er bei bestimmten Gelegenheiten hält (so etwa Thür 2010). Er ist als weisungsunabhängige Behörde zwar keiner anderen Behörde Rechenschaft schuldig, jedoch der Öffentlichkeit, die ihn finanziert. Das Fehlen einer zusammenfassenden und bilanzierenden Perspektive in den Jahresberichten zum Datenschutz allgemein und zu seinem Wirken im Besonderen erweckt gegen aussen bis zu einem gewissen Grad das Bild einer Behörde, die ohne klares Konzept, inputorientiert und zufällig punktuell agiert, obwohl dies – soweit es im Rahmen dieser Evaluation abzuklären war – nicht zuzutreffen scheint.

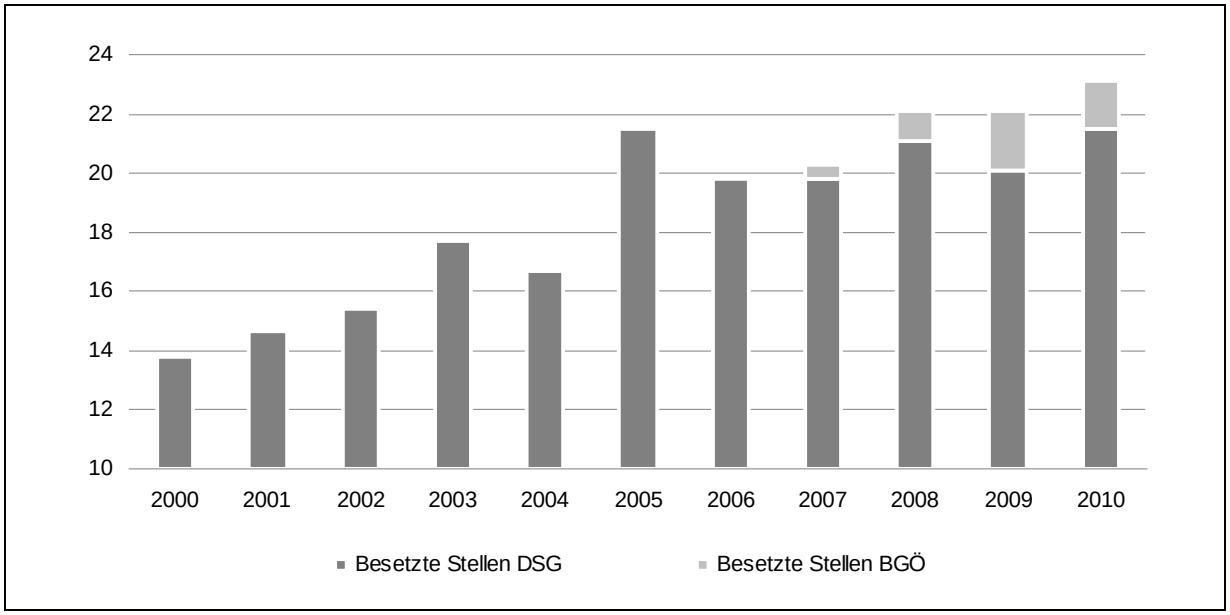
11.3 Ressourcensituation

In diesem Abschnitt wird auf die Ressourcen des EDÖB zur Bewältigung seiner Aufgaben eingegangen. Der EDÖB verfügt gemäss Art. 26 Abs. 3 DSG selbständig über sein Budget und teilt demzufolge auch die Ressourcen selbständig zwischen den Aufgaben aus dem BGÖ und dem DSG auf.

11.3.1 Personalbestand

Der Personalbestand des EDÖB hat sich im letzten Jahrzehnt vergrössert. Der Hauptanteil des Stellenanstiegs erfolgte, basierend auf Beschlüssen im Jahr 2004, insbesondere 2005 (vgl. Abbildung 11-2). Die seither vom EDÖB eingebrachten Anträge auf zusätzliche Stellenprozente sind nicht oder nur minderheitlich bewilligt worden. Der zusätzliche Aufwand durch das BGÖ beispielsweise war in der Botschaft des Bundesrats auf drei bis dreieinhalb Stellen veranschlagt worden (Bundesrat/BBl 2003 2035), sie wurden nach Inkrafttreten des Gesetzes im Jahr 2006 jedoch nie bewilligt. Die Finanzierung der Personalausgaben für den Vollzug des BGÖ wurde so durch anderweitige, kleinere Budgeterhöhungen und mithin teilweise auf Kosten der datenschützerischen Aufgaben sichergestellt. Während zweier Jahre wurde dem EDÖB ein zusätzlicher Beitrag aus den Mitteln der Bundeskanzlei gewährt. 2009 wurden dem EDÖB im Zusammenhang mit den neuen Aufgaben aus dem Beitritt zu den Abkommen von Schengen und Dublin drei zusätzliche Stellen bewilligt.

Abbildung 11-2: Entwicklung des Personalbestands des EDÖB



Quelle: EDÖB. Personalbestand jeweils anfangs Jahr. Eigene Darstellung.

Mitte 2010 verfügte der EDÖB über 24.6 Stellen, was einer Aufstockung gegenüber anfangs 2010 entspricht. Neben der Direktion (3.6 Stellen) und dem Administrativpersonal (2.4 Stellen) waren

die Stellen überwiegend von Juristen besetzt (12.6 Stellen, davon 1.6 Stellen für das BGÖ), ergänzt um 4.4 Stellen für Informatiker und 1.6 für Information. Im internationalen Vergleich ist die personelle Ausstattung des EDÖB als eher gering anzusehen, wobei aufgrund der Unterschiede bezüglich Zuständigkeitsbereichen (private und öffentliche Bearbeiter, föderale Ebenen), aufgrund der Aufgaben und aufgrund der Grösse der Länder der Vergleichbarkeit der Personaletats enge Grenzen gesetzt sind.[243]

11.3.2 Einschätzungen zu den Ressourcen

Die Befragten beim EDÖB bezeichnen die Ressourcensituation als unbefriedigend. Zwar hätten Massnahmen zur Effizienzsteigerung eine gewisse Entlastung gebracht. So versucht der EDÖB durch eine Beschränkung der Anrufzeiten auf seine Hotline auf täglich zwei Stunden die telefonischen Anfragen zu kanalisieren und den Mitarbeitenden den Rücken in der übrigen Arbeitszeit freizuhalten. Auch verzichtet er seit einigen Jahren auf die individuelle Bearbeitung von Einzelanfragen, sondern antwortet mit Standardbriefen (vgl. Ziffer 12.2.4). Gleichwohl zwinge die aktuelle Ressourcensituation zu einer starken Priorisierung und es komme vor, dass Geschäfte auf die lange Bank geschoben werden müssten – sprich: in Kategorie B versetzt werden –, die eigentlich zwingend bearbeitet werden müssten. Einzelne Geschäfte wie eine grössere Sachverhaltsabklärung würden bisweilen die Ressourcen einzelner Fachbereiche stark absorbieren (vgl. insbesondere Fallstudien *Google Street View* und *Logistep*), und der Aufwand hierfür sei nicht immer gut planbar. Insbesondere dürfte es schwierig sein abzusehen, ob der Bearbeiter allfällige Empfehlungen umsetzt oder der Gang vor das Gericht notwendig wird.

Auch die rechtswissenschaftliche Literatur kommt zum Schluss, der EDÖB verfüge für eine umfassende Wahrnehmung seiner Aufgaben über (zu) wenig Personal (Huber 2006: 368-370, mit Verweisen auf weitere Literatur und behördliche Berichte). Die Interviewpartner, welche sich zu den Ressourcen eine Einschätzung zutrauten (Rechtsexperten und Interessenvertreter von Organisationen der Betroffenen), gaben allesamt zu Protokoll, die Ausstattung des EDÖB sei schwach.

Vor dem Hintergrund der Ressourcenausstattung sind auch drei Urteile des Bundesverwaltungsgerichts bemerkenswert (BVerwG A-363/2010, BVerwG A-6032-2009, BVerwG A-75-2009). In diesen Urteilen gibt das Gericht jeweils einer Beschwerde wegen Rechtsverzögerung durch den EDÖB Recht. Dieser hatte auf Begehren von Bürgern im Rahmen des Öffentlichkeitsgesetzes BGÖ nicht fristgerecht reagiert, und dies auch mit Ressourcenmangel begründet. Das Gericht anerkannte diese Argumentation nicht und wies den EDÖB an, seiner gesetzlichen Verpflichtung nachzukommen. In zwei von drei Fällen brachte das Gericht sein Urteil dem Bundesrat zur Kenntnis, der wie ausgeführt sowohl hinsichtlich der Wahl als auch des Budgets des EDÖB eine zentrale Rolle spielt.

[243] Personaletats der nationalen Datenschutzbehörden in ausgewählten Ländern 2010 (gemäss Angaben des EDÖB): Irland (22 Stellen), Kroatien (26), Litauen (30), Schweden (43), Belgien (54), Deutschland (77.5), Niederlande (85), Tschechien (102), Polen (121), Frankreich (157), Grossbritannien (319).

11.4 Zusammenarbeit und Koordination mit anderen Akteuren

Der EDÖB arbeitet mit verschiedenen Akteuren zusammen, die Aufgaben im Bereich des Datenschutzes übernehmen. Im Folgenden soll dabei die Zusammenarbeit mit ausländischen und inländischen Datenschutzbehörden (Art. 31 Abs. 1 Bst. c DSG) sowie mit Organisationen zum Schutz der Betroffenen behandelt werden. Die folgenden Ausführungen basieren auf der Literatur und Dokumentationen des EDÖB, verschiedenen Interviews sowie auf den durchgeführten Fallstudien.

11.4.1 Internationale Zusammenarbeit

Die internationale Zusammenarbeit nimmt gemäss den Aussagen der Interviewpartner beim EDÖB eine wichtige, und in Zukunft eine immer wichtigere, Rolle ein. Die zunehmende Bedeutung ergibt sich primär aus den Folgen der fortschreitenden internationalen Verknüpfung der Datenbearbeiter und der technologischen Entwicklungen, die nicht vor den Landesgrenzen halt machen und zunehmend länderübergreifende Problemstellungen hervorbringen. Die Zusammenarbeit mit ausländischen Datenschutzbehörden soll im Falle transnationaler Datenbearbeitungen ermöglichen, abgestimmte Antworten zu erteilen. Zu diesem Zweck beteiligt sich der EDÖB in verschiedenen Gremien und Formen der internationalen Zusammenarbeit:

- Internationale Konferenz der Datenschutzbeauftragten
- Europäische Konferenz der Datenschutzbeauftragten
- Frankophone Vereinigung der Datenschutzbehörden
- Europarat: Beratendes Komitee der Datenschutzkonvention
- Gemeinsame Kontrollinstanzen Schengen und Eurodac (Dublin)

Bei der Einschätzung, was die internationale Zusammenarbeit für den Datenschutz tatsächlich bringt, sehen die Interviewpartner beim EDÖB im Wesentlichen zwei konkrete Punkte, in denen die Schweiz vom internationalen Austausch profitiert. Erstens bilde dieser eine nützliche Informationsbörse: Der EDÖB erhalte Hinweise, was in anderen Ländern bezüglich welcher Probleme unternommen werde; zudem könne er zu bestimmten Fragen von den Vorarbeiten anderer Länder profitieren. So kläre er beispielsweise beim Verfassen von Erläuterungen ab, welche Informationsprodukte international bereits bestehen. Zweitens bestehe das Interesse an einem koordinierten Vorgehen in Fragen des Datenschutzes. Einerseits sei dies notwendig zur Schaffung gemeinsamer Normen für grenzüberschreitende Fragen. Andererseits sei es angesichts des regen Datenaustauschs zwischen der Schweiz und den Ländern der EU für die Schweiz wichtig, die eigene Praxis auf jene der Europäischen Union abzustimmen. Im Fallbeispiel *Logistep* sah sich der EDÖB aufgrund von Beschwerden von Datenschutzbeauftragten umliegender Länder zum Handeln veranlasst: Andernfalls hätte seines Erachtens die Schweiz gegenüber der EU den Eindruck erweckt, dass eine Datenbearbeitung, die in vielen EU-Staaten als widerrechtlich betrachtet wird, in der Schweiz toleriert werde.

Trotz der zunehmenden internationalen Koordination der Datenschutzbehörden erfolgt die Durchsetzung von Ansprüchen der Betroffenen weiterhin in den einzelnen Nationalstaaten. Gleichzeitig zeigt sich z.B. im Fall *Google Street View*, dass die Koordination zwischen den Datenschutzbehörden in konkreten Anwendungsfällen noch nicht immer zu einheitlichen Lösungsansätzen führt und keine klare Arbeitsteilung besteht (vgl. Baeriswyl 2009). Gerade gegenüber multinationalen Anbietern dürfte indes ein koordiniertes Vorgehen auch im Bereich der Aufsicht sinnvoll sein.

11.4.2 Zusammenarbeit mit kantonalen Datenschutzbehörden

Die Zusammenarbeit zwischen dem EDÖB und den kantonalen Datenschutzbeauftragten ist im Rahmen dieser Evaluation nicht systematisch behandelt worden. Insbesondere wurden keine Vertreter kantonaler Datenschutzbehörden befragt. Thematisiert werden kann kurz die grundsätzliche Aufgabenteilung zwischen Bund und Kantonen beim Datenschutz. Von Interesse ist dabei primär der privatrechtliche Bereich; die Zuständigkeit des EDÖB für Bundesorgane sowie die Zuständigkeit der kantonalen Datenschutzstellen für kantonale und kommunale Anliegen dürften kaum Anlass zu Diskussionen bieten.

Bezüglich der Beratung und Aufsicht von Firmen argumentieren die Befragten beim EDÖB, dass es sinnvoll sei, wenn diese Aufgaben im Zuständigkeitsbereich des EDÖB lägen. Nur so könne gewährleistet werden, dass Unternehmen in allen Kantonen der Schweiz identische Informationen erhielten und ihre Datenbearbeitungen nach einheitlichem Massstab beurteilt würden. Eine kantonale Zuständigkeit beinhalte demgegenüber ein gewisses Risiko, dass je nach Kanton unterschiedliche Regelungen gälten, was nicht im Interesse der Wirtschaft liegen könne.

Im Bereich der Beratung von Privatpersonen nannte hingegen ein befragter Rechtsexperte die grössere Bürgernähe sowie die Entlastung des nationalen Datenschutzbeauftragten als Gründe, die für eine Zuweisung dieser Aufgaben an die Kantone sprächen. Das Fallbeispiel *Baubranche* und (allerdings zahlenmässig bescheidene) Ergebnisse der Bevölkerungsbefragung liefern Hinweise, dass der jeweilige kantonale Datenschutzbeauftragte den Betroffenen und Bearbeitern je nach dem näher stehen könnte. Von Seiten des EDÖB hält man dem entgegen, dass gerade der Kontakt mit der Bevölkerung und den Bearbeitern im Rahmen der Beratung wertvolle Hinweise liefere, wo mögliche Probleme lägen.

Eine abschliessende Bewertung der Kompetenzaufteilung zwischen Bund und Kantonen ist aufgrund dieser wenigen Hinweise nicht möglich. Erwähnt sei ergänzend, dass in Deutschland die Datenschutzbehörden der Bundesländer für die Datenbearbeitungen von Privatpersonen zuständig sind. In den meisten im internationalen Rechtsvergleich berücksichtigten Ländern ist die nationale Behörde das einzige Aufsichtsorgan für den Datenschutz (SIR 2010: 34)

11.4.3 Organisationen zum Schutz der Betroffenen

Die Interviewpartner sehen die Rolle von Organisationen zum Schutz der Betroffenen heute insgesamt als schwach an. Von einer befragten Person wird der EDÖB als einziger Akteur in diesem Bereich wahrgenommen. Auch die Befragten beim EDÖB messen diesen Organisationen

insgesamt keine grosse Bedeutung zu. Sie weisen darauf hin, dass in der Schweiz keine eigentliche Datenschutzorganisation bestehe. Die befragten Interessenorganisationen selber geben an, dass der Datenschutz für sie zwar zunehmend an Bedeutung gewinne, ihnen aber in der jetzigen Situation das Know-how noch fehle. Jedoch handle es sich beim Datenschutz um ein Gebiet sei, in das man künftig vermehrt Zeit investieren wolle und müsse. Auch die Befunde der Bevölkerungsumfrage deuten in die Richtung, dass diese Organisationen für die Bürger keine wichtige Anlaufstelle sind (vgl. Ziffer 8.2.2).

Bei der Frage, wo die Interviewpartner Möglichkeiten für diese Organisationen sehen, sich in die Diskussion einzubringen, wird sowohl auf die Förderung als auch auf die Durchsetzung des Datenschutzes verwiesen. Ein Teil der befragten Personen sieht ein Potenzial für die Bewusstseinsbildung bei den Betroffenen. In zwei Interviews wurde die Möglichkeit diskutiert, Organisationen zum Schutz der Betroffenen griffigere Rechte in die Hand zu geben, um im Falle von Datenschutzverletzungen vorgehen zu können. Dies wird insofern als eine sinnvolle Möglichkeit erachtet, weil sich für den Einzelnen kaum lohne, den Rechtsweg zu beschreiten.

11.4.4 Einbezug von Ressourcen der Bundesorgane und Privater Bearbeiter

Gemäss Art. 23 VDSG müssen die Bundeskanzlei und die Departemente mindestens je einen Datenschutzberater bezeichnen. Dieser hat die Aufgabe, die verantwortlichen Organe und Benützer zu unterstützen, die Information und Ausbildung der Mitarbeiter zu fördern und beim Vollzug der Datenschutzvorschriften mitzuwirken. Der Verkehr zwischen den Bundesorganen und dem EDÖB erfolgt laut Art. 23 VDSG über die Datenschutzberater. Hinsichtlich der Ausstattung und organisatorischen Einbettung ihrer Datenschutzberater sind die Departemente frei.

Den Evaluatoren ist keine Übersicht bekannt, welche Aufschluss darüber gibt, wie die einzelnen Departemente ihre Datenschutzberater ausstatten und welche Einflussmöglichkeiten sie ihnen zugestehen. Aufgrund der wenigen durchgeführten Gespräche mit Datenschutzberatern des Bundes haben sich diesbezüglich Unterschiede gezeigt, die jeweils mit den konkreten Tätigkeiten der Bundesstelle begründet wurden. Die Befragten beim EDÖB stellen bezüglich Ausstattung und Bedeutung der Datenschutzberater grosse Unterschiede fest. Einzelne Departemente beschränkten sich auf die vorgegebene Mindestanforderung, in anderen Departementen existierten auch auf Ebene von Bundesämtern Datenschutzbeauftragte. Nach seiner Erfahrung ist auch die Bedeutung der Berater in den Ämtern sehr unterschiedlich. Bisweilen würden die Datenschutzberater bei datenschutzsensitiven Projekten umgangen, in anderen Amtsstellen seien sie ein fester Bestandteil der internen Planungsabläufe. Noch zu oft werde an ihn die Erwartung herangetragen, dass er sich an der Erarbeitung von Lösungen stark beteilige, kritisieren die befragten Mitarbeitenden beim EDÖB. Dies übersteige jedoch seine Ressourcen und entspreche auch nicht seiner Rolle.

Beim EDÖB betonten die Interviewpartner nicht zuletzt, dass sie ihre Rolle nicht in der Rolle der ersten Anlaufstelle für die Departemente sieht. Erst wenn ein Problem departementsintern nicht mehr gelöst werden könne, sollte der EDÖB ins Spiel kommen. Die befragten Datenschutzberater aus der Bundesverwaltung (zwei auf Stufe Amt, einer auf Stufe Departement) gelangen zu etwas anderen Einschätzungen. Zwei Interviewpartner kritisieren, dass der EDÖB

kaum für Beratungen zur Verfügung stehe; in einem Fall scheint die Zusammenarbeit gut zu funktionieren. Die Antworten weisen ausserdem darauf hin, dass man nicht mit jeder Kleinigkeit zum EDÖB gehe, sondern dass der departementsinterne Spielraum ausgenutzt werde.

Die Verallgemeinerbarkeit der Aussagen der befragten Datenschutzbearbeiter ist aufgrund der tiefen Fallzahl nicht möglich. Klar scheint jedoch, dass sich die Beratungstätigkeit des EDÖB schon angesichts seiner knappen Ressourcen auf zentrale Projekte der Bundesverwaltung zu fokussieren hat. Zudem ist der Vorschrift, wonach der Verkehr zwischen den Bundesorganen und dem EDÖB via die Datenschutzberater zu erfolgen hat (Art. 23 VDSG), konsequent nachzuleben. Dies vereinfacht den Kommunikationsfluss zwischen Verwaltung und EDÖB und stärkt die Datenschutzberater.

Die Arbeitsteilung zwischen Bundesorganen und dem EDÖB ist bereits im Rahmen früherer Untersuchungen thematisiert worden (GPK-N 2003, EFK 2007). Insgesamt deuten die wenigen Abklärungen im Rahmen dieser Evaluation darauf hin, dass die gegenseitigen Erwartungen zwischen Bundesorganen und EDÖB hinsichtlich der Rollenteilung zumindest punktuell immer noch auseinanderklaffen.

Im Gesetz sind mit der 2008 in Kraft getretenen Revision Anreize geschaffen worden, die Datenschutzstrukturen auf Seiten der privaten und öffentlichen Datenbearbeiter zu stärken. So können Datenbearbeiter auf die Anmeldung von Datensammlungen verzichten, wenn sie selbst einen Datenschutzverantwortlichen bezeichnen und diesen beim EDÖB anmelden (Art. 11a Abs. 5 Bst. e DSG). Mit der Zertifizierung (Art. 11 DSG) kann ebenfalls auf privatem Weg der Datenschutz gestärkt werden. Im Moment kann noch nicht beurteilt werden, inwieweit diese neuen gesetzlichen Möglichkeiten von eigenverantwortlichem Datenschutz den EDÖB entlasten. Auch die teilweise bestehenden privaten Datenschutzberatungsangebote für die Bearbeiter nimmt der EDÖB nicht als Entlastung wahr.

Als positiv zu bewerten ist das Entstehen von privaten Fachorganisationen, in denen sich die für den Datenschutz zuständigen Personen der Datenbearbeiter treffen und weiterbilden und die auch einen Austausch mit dem EDÖB pflegen. In der Deutschschweiz handelt es sich um den Verein Unternehmensdatenschutz (VUD), in der Romandie um die Association des Professionnels de la Protection des Données (APPD).

12 Aktivitäten des EDÖB

In diesem Kapitel werden die wichtigsten gesetzlichen Aufgaben des EDÖB untersucht. Zunächst wird ein Überblick über die Bekanntheit des EDÖB und seine Aktivitäten geliefert, die nachfolgenden Abschnitte fokussieren auf die wichtigsten Aktivitäten, so auf die Beratung, auf die Aufsicht und auf die Information. In einem separaten Abschnitt wird auf Zusammenhänge zwischen den Hauptaktivitäten eingegangen. Der abschliessende Abschnitt behandelt die Stellungnahmen des EDÖB im Rahmen der Rechtsetzung.

12.1 Bekanntheit und Aktivitäten des EDÖB im Überblick

Dieser Abschnitt zeigt überblicksartig, welche Anteile seiner Tätigkeit der EDÖB auf die Bereiche der Aufsicht, der Information und der Beratung verwendet. Er gibt auch Aufschluss über die Themengebiete, in denen sich der EDÖB stark engagiert. Als Datengrundlage dient die quantitative Auswertung des Geschäftsverwaltungssystems, ergänzt mit Interviewaussagen von Mitarbeitern des EDÖB. Zuvor wird anhand der Erkenntnisse aus der Bevölkerungsumfrage und der Interviews mit den Datenbearbeitern und Experten auf die Bekanntheit des EDÖB eingegangen.

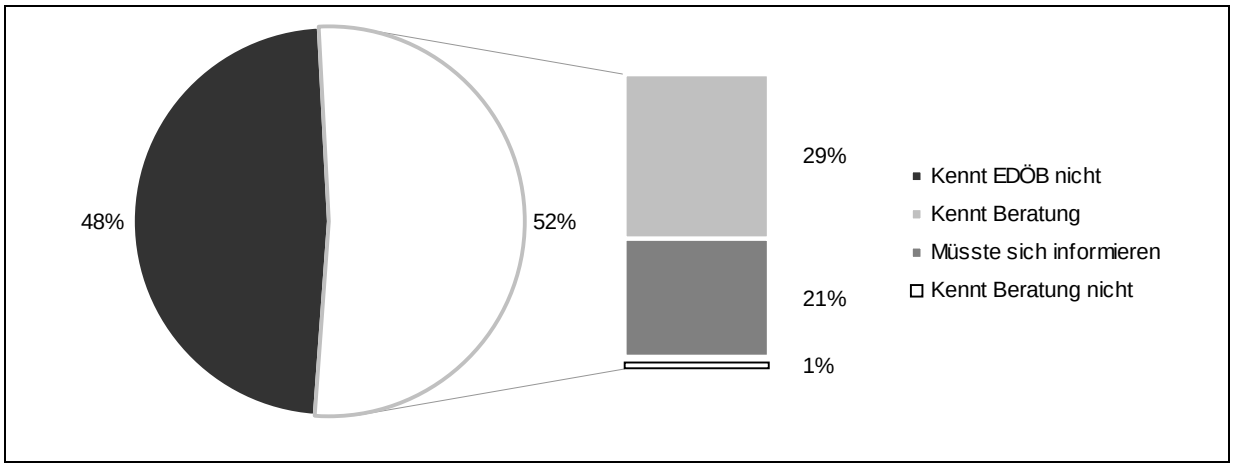
12.1.1 Bekanntheit des EDÖB

Bekanntheit bei der Bevölkerung insgesamt

Die Bekanntheit des EDÖB bei der Bevölkerung wurde in der Umfrage analog zur Bekanntheit des DSG erfragt. Abbildung 12-1 zeigt, dass der EDÖB weniger bekannt ist als das DSG. 48% der Befragten gaben an, vom EDÖB bisher noch nie gehört zu haben. Von jenen Befragten, die den EDÖB kennen, zeigt sich dafür gut die Hälfte richtigerweise überzeugt, dass sie sich direkt durch den EDÖB beraten lassen können. Bezogen auf alle Befragten sind es 29%. 21% der Befragten geben an, sie müssten sich zuerst informieren.

Im Rahmen der Eurobarometer-Umfrage erwiesen sich die nationalen Datenschutzbehörden in den EU-Ländern als relativ unbekannt. Durchschnittlich kannten bloss 28% die Behörde. Insofern kann die schweizerische Bevölkerung als vergleichsweise gut informiert bezeichnet werden. Von denjenigen EU-Bürgern, die ihre Behörde kennen und deren Behörde die Betroffenen berät, scheint im Durchschnitt ein ähnlicher Anteil diese Aufgabe zu kennen wie in der Schweiz.

Abbildung 12-1: Kenntnis des EDÖB und seiner Beratungsfunktion



N = 1014. Lesehilfe: 52% der Befragten (weisse Fläche) haben vom EDÖB schon gehört. In dieser Gruppe bejahten 29% die Zusatzfrage, ob man sich bei diesem direkt beraten lassen könne. 21% gaben bei der Zusatzfrage an, sie müssten sich zuerst informieren, 1% verneinte die Möglichkeit des Gerichtswegs (keine Antwort/weiss nicht: 1%). Genaue Fragestellung vgl. Anhang 2.

Bekanntheit in gesellschaftlichen Untergruppen

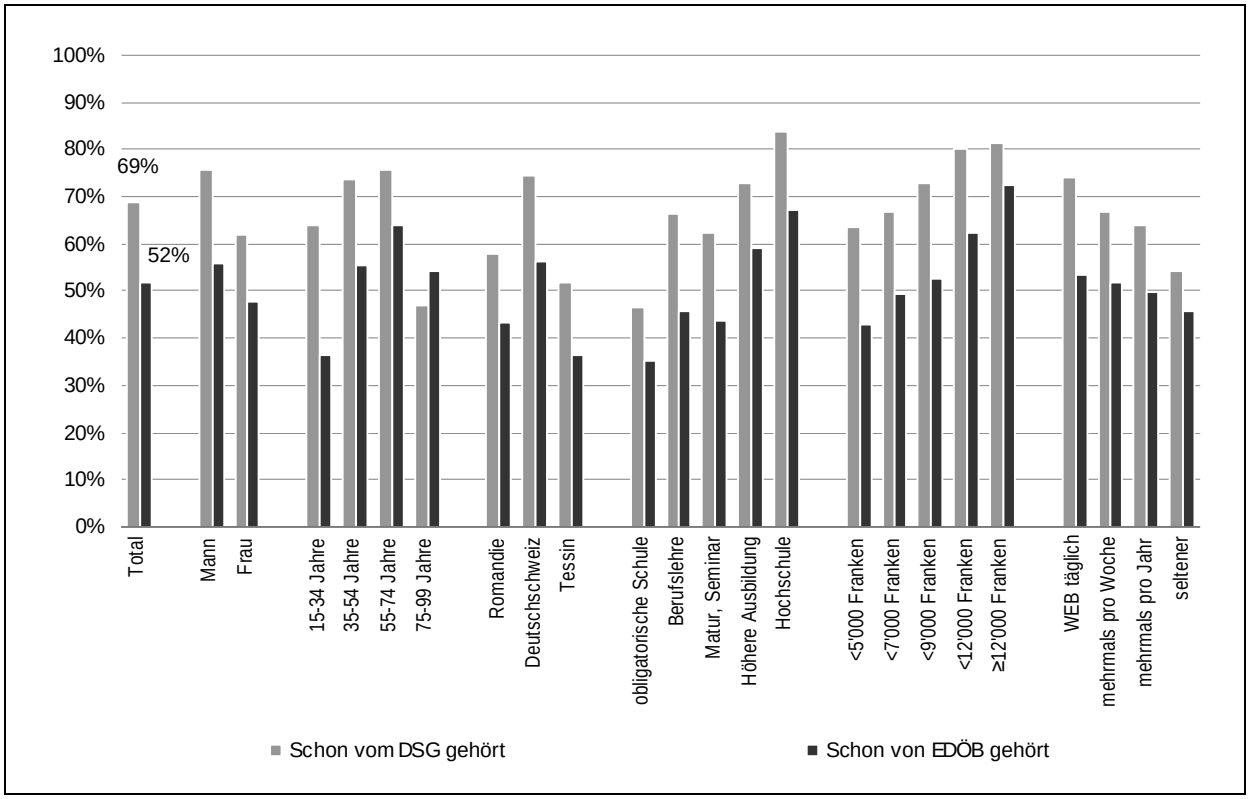
Hinsichtlich der Bekanntheit des EDÖB bestehen ähnlich wie beim DSG deutliche Unterschiede zwischen den verschiedenen soziodemographischen Gruppen. Der Befund, wonach der EDÖB weniger bekannt ist als das Gesetz, zeigt sich dabei durchgehend, ausser in der Gruppe der 75-99jährigen Befragten. Im Übrigen lässt Abbildung 12-2 klare Tendenzen erkennen. Männer haben vom DSG und vom EDÖB etwas häufiger gehört als Frauen, Personen mit hohem Bildungsniveau und hohem Einkommen häufiger als Personen mit niedrigem Bildungsniveau und niedrigem Einkommen. Dabei kann festgehalten werden, dass von den untersuchten Merkmalen zwischen den Bildungsgruppen die stärksten Unterschiede bestehen: 46% der Personen, deren höchster Abschluss die obligatorische Schule ist, ist das DSG bekannt, 35% kennen den EDÖB; von den Hochschulabsolventen gaben 84% an, sie kennten das DSG und 67% den EDÖB.

Auch regelmässigen Nutzern des Internet ist der EDÖB (wie das DSG) häufiger bekannt als Personen, die sich selten im Netz bewegen. Sprachregional gesehen sind die Bekanntheit des Gesetzes und des EDÖB im Tessin und in der Romandie tiefer als in der Deutschschweiz. Hinsichtlich des Alters zeigen sich zwar deutliche Unterschiede, doch gibt es keinen eindeutigen Trend. Bis zur Gruppe der 55-74jährigen steigt die Bekanntheit an, in der Gruppe der 75-99 ist sie wieder etwas tiefer. Alle beschriebenen Gruppenunterschiede sind statistisch signifikant mit einer Irrtumswahrscheinlichkeit von maximal 10%.

Die Resultate zeigen somit, dass nicht erwartet werden kann, die Bevölkerung kenne den EDÖB und seine Aufgaben sehr gut. Insbesondere bestehen teils recht deutliche Gruppenunterschiede. Bei bestimmten gesellschaftlichen Gruppen (Junge, Seniorinnen und Senioren, Tessinerinnen und Tessiner, Personen mit niedriger Bildung) muss davon ausgegangen werden, dass jeweils eine deutliche Mehrheit der Bevölkerung im Falle eines Problems nicht an eine mögliche Hilfestellung durch den EDÖB denkt. Auch bei einem Missbrauch ihrer persönlichen Daten erwägen gemäss

der Umfrage die wenigsten Personen, den EDÖB (oder auch eine kantonale Datenschutzbehörde) zu konsultieren. Die weit über tausend Kontaktaufnahmen pro Jahr, die der EDÖB in seinen früheren Jahresberichten noch regelmässig auswies (vgl. etwa EDSB 2001/2002) und die rege Frequentierung seiner Homepage (vgl. Ziffer 12.5) können somit nicht darüber hinwegtäuschen, dass ein grosser Teil der Bevölkerung ihre Datenschutzbehörde nicht oder nicht gut kennt. Die Probleme, auf die der EDÖB aufgrund von direkten Anfragen Betroffener stösst, bilden somit vermutlich bloss die Spitze des Eisbergs. Gleichwohl dürften diese Kontaktaufnahmen für den EDÖB wertvolle Hinweise liefern, in welche Richtung er seine Aktivitäten zu lenken hat.

Abbildung 12-2: Bekanntheit des EDÖB und des DSG, nach sozialen Gruppen



N = 1014 Befragte. Exakte Fragestellung vgl. Anhang 2.

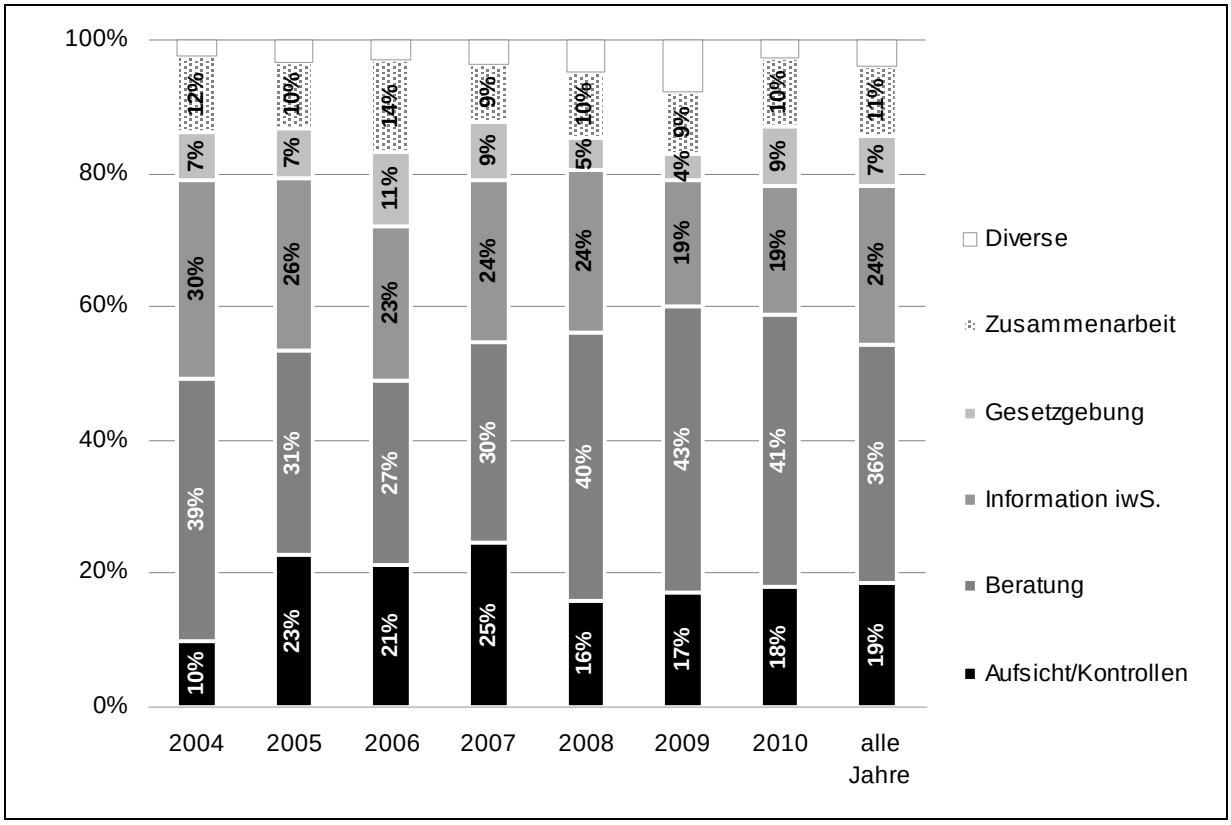
12.1.2 Gewichtung der verschiedenen EDÖB-Aktivitäten

Das Gesetz verpflichtet den EDÖB schwergewichtig auf die Beratung, die Aufsicht und die Informationstätigkeit. In der jüngeren Vergangenheit hat sich der EDÖB Interviewaussagen zufolge bemüht, der Aufsichtstätigkeit insbesondere über private Datenbearbeiter ein höheres Gewicht einzuräumen. Ermöglichen sollte dies einerseits die Rationalisierung der Beratung Betroffener, indem diese z.B. heute mittels Standardantworten auf den Rechtsweg verwiesen werden, wenn sie ihre Rechte verletzt glauben. Andererseits versuchte der EDÖB, seinen Aufwand für die Beratung von Bundesbehörden zu reduzieren.

Abbildung 12-3 zeigt die tatsächliche Entwicklung bezüglich der Tätigkeitsanteile seit dem Jahr 2004. Die Auswertung basiert auf dem Geschäftsverwaltungssystem des EDÖB, in dem die Mit-

arbeitenden ihre Arbeitszeit gegliedert nach Tätigkeit und Sachbereich eintragen. Trotz ihrer Unschärfen (vgl. Einleitung zu Teil IV) vermittelt die Daten einen Eindruck über das relative Gewicht der verschiedenen Aufgaben. Die Auswertung zeigt, dass der EDÖB für seine gesetzlich vorgegebenen Kernaufträge der Aufsicht, Beratung und Information regelmässig zwischen 70 und 80% seiner produktiven Zeit aufgewendet hat (administrative Tätigkeiten sind in der Statistik nicht enthalten). Der grösste Anteil entfällt dabei auf die Beratung, nämlich zwischen 27% (2006) und 43% (2009). Bei der Aufsicht sind zwei Phasen klar unterscheidbar. Bis 2007 beträgt ihr Aufwand zwischen 20 und 25% (der Wert von 2004 ist aufgrund einer damaligen Änderung der Codierung im Geschäftsverwaltungssystem wenig aussagekräftig). Danach liegt er immer unter 20%.

Abbildung 12-3: Tätigkeitsanteile des EDÖB, nach gesetzlichen Aufgaben



Quelle: Geschäftsverwaltungssystem des EDÖB, eigene Berechnungen. Die Amtsjahre des EDÖB dauern jeweils vom 1.4. bis am 31.3. des folgenden Jahres. „2004" bezeichnet das Amtsjahr 2003/04. Die errechneten Tätigkeitsanteile basieren auf der aufgewendeten Zeit in Stunden. Information i.w.S. umfasst neben der Publikationstätigkeit auch den Zeitaufwand für die Ausbildung und Konferenzen.

Die Absicht, die Aufsichtstätigkeit auszudehnen, konnte somit nur partiell umgesetzt werden. Der Rückgang der Aufsicht und der Zuwachs der Beratung ab 2008 werden vom EDÖB vorab mit strategischen Entscheidungen des EDÖB und Bedürfnissen der Bearbeiter begründet. Mitte der 2000er Jahre wurde wie erwähnt beschlossen, sich stärker auf die Aufsichtstätigkeit zu konzentrieren und insbesondere die Beratung beim Bund stark zu reduzieren, was die relativ hohen Werte für die Aufsicht der Jahre 2005 bis 2007 erklärt. Später habe der EDÖB auf Drängen der

Bundesbehörden die Beratungstätigkeit bei den Bundesämtern wieder gesteigert und seine Präsenz in Arbeitsgruppen und Begleitgruppen von Projekten wieder erhöht. Als weiterer Grund wird die Personalfluktuation erwähnt, welche dazu geführt habe, dass einzelne Aufsichtsprojekte für eine bestimmte Zeit sistiert waren.[244]

Die interviewten Datenbearbeiter nehmen den EDÖB eher als Berater denn als Aufsichtsorgan wahr. Die Interessenvertreter von Arbeitnehmern und Konsumenten sowie ein Rechtsexperte plädierten für eine Stärkung der Aufsicht; einem Rechtsexperten zufolge sind der EDÖB (und das DSG) für Unternehmen zuwenig furchteinflössend, um diese zu zwingen, sich an die gesetzlichen Regeln zu halten. Er hält also das Sanktionsrisiko für gering. Der andere befragte Rechtsexperte betonte die Wichtigkeit der Beratung. Unter den Technologieexperten sind die Meinungen geteilt.

Die Vertreter des EDÖB selbst beurteilten im Interview den Anteil der Aufsicht als noch zu niedrig. Sie geben sich zuversichtlich, dass er künftig gesteigert werden könne. Die Aufsicht wird als wichtig eingestuft, weil dadurch der Öffentlichkeit signalisiert werde, dass der EDÖB präsent sei. Seitens des EDÖB erhofft man sich dadurch auch einen präventiven Effekt auf andere Bearbeiter.

Für die Information hat der EDÖB in den vergangenen sieben Amtsjahren insgesamt am zweitmeisten Arbeitszeit aufgewendet (primär Internet, Ausbildung und Konferenzauftritte), wobei ihr Stellenwert rückläufig ist und in den letzten beiden Amtsjahren noch bei 19% lag. Die Interviewpartner erklärten diesen Rückgang im Interview mit einer bewussten Akzentverschiebung: Nachdem in früheren Jahren viel Zeit für den Ausbau des Informationsangebots auf dem Internet investiert worden sei, werde heute die Homepage regelmässig aufdatiert, was zwar immer noch einen beachtlichen Aufwand bedeute, aber weniger ressourcenintensiv als die Aufbauphase der Seite sei.

Von den übrigen gesetzlichen Aufgaben nehmen die Stellungnahmen zu Gesetzesprojekten mit 5 bis 10% einen namhaften Zeitaufwand in Anspruch. Übertroffen werden sie von der Zusammenarbeit mit kantonalen und ausländischen Datenschutzbehörden. Die Bewilligung von Zertifizierungsstellen, das Register der Datensammlungen und die Bearbeitung von Gesuchen im Rahmen der indirekten Auskunft (betrifft Einträge in Datenbanken des Fedpol) beanspruchen nur wenig Ressourcen (Kategorie „Diverse“).

12.1.3 Ressourceneinsatz des EDÖB nach Sachgebieten

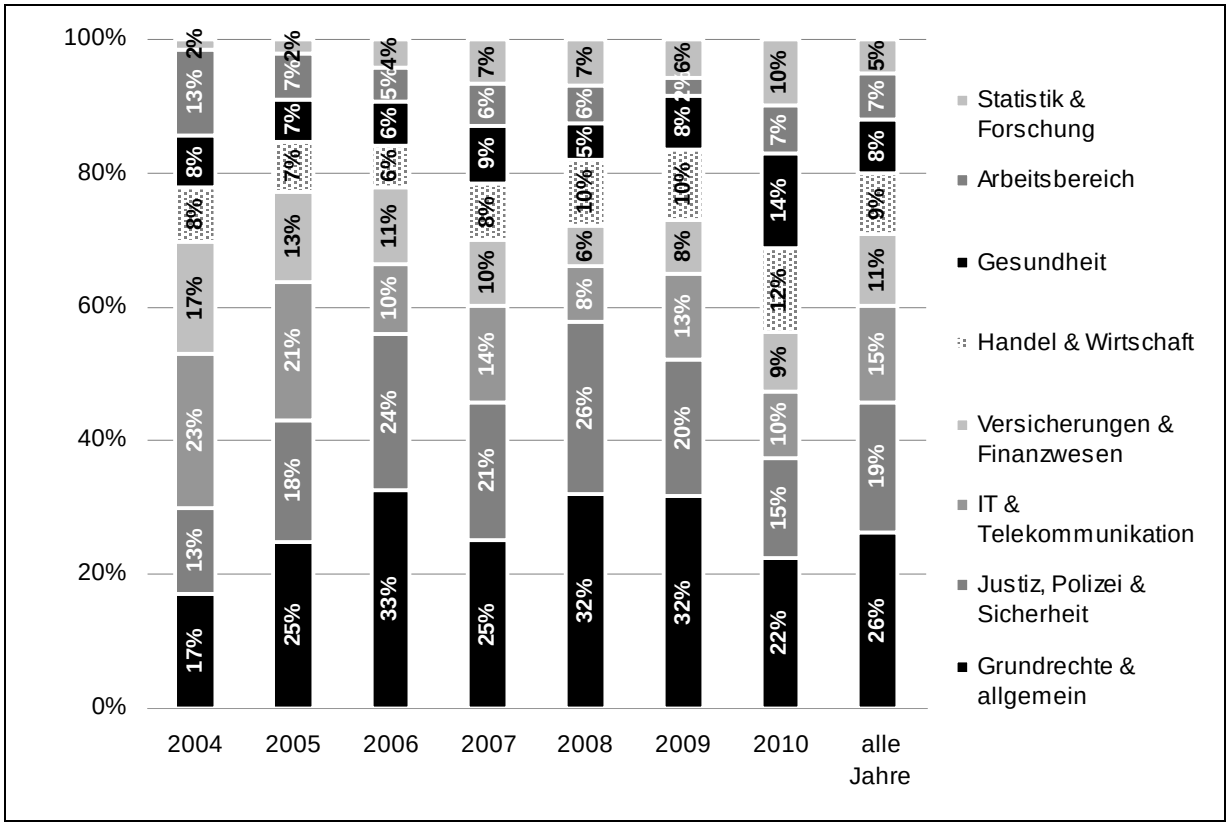
Abbildung 12-4 gibt einen Überblick über die Tätigkeitsanteile des EDÖB in verschiedenen Sachgebieten. Die Auswertung basiert auf der Zuordnung des EDÖB, wobei teils kleine Kategorien zusammengefasst wurden. Im Durchschnitt konnten rund ein Viertel der aufgewendeten Stunden keiner vorgegebenen Kategorie zugeordnet werden oder fielen (zum kleineren Teil) in

[244] Eine Auswertung, welche die Zeitanteile der Aktivitäten nach privaten und öffentlichen Bearbeitern/Betroffenen aufschlüsselt, ist anhand der zur Verfügung stehenden Daten nicht möglich. Eine Gliederung nach Privat/Bundesorgan führt der EDÖB nur bei der Beratung durch.

die Kategorie Grundrechte; solche Geschäfte befassen sich mit grundlegenden Aspekten des Datenschutzes, die von themenübergreifender Bedeutung sind.

Die Aktivitäten des EDÖB decken eine breite Palette an Themen ab. Den grössten Tätigkeitsanteil verbuchen die Kategorien „Justiz, Polizei und Sicherheit“ (inklusive Verteidigung), gefolgt von „IT und Telekommunikation“. Auffallend ist, dass die Bedeutung der einzelnen Sachbereiche über die Zeit recht stark schwankt. Es sind kaum deutliche Trends erkennbar. Die Schwankungen dürften im Einzelnen teils die Folge von bewussten Entscheidungen des EDÖB sein, überwiegend spiegeln sie aber wohl die Schwankungen auf Seiten der Anliegen, die von aussen an den EDÖB herangetragen werden.

Abbildung 12-4: Tätigkeitsanteile des EDÖB, nach Sachgebieten



Quelle: Geschäftsverwaltungssystem des EDÖB, eigene Berechnungen. Die Amtsjahre des EDÖB dauern jeweils vom 1.4. bis am 31.3. des folgenden Jahres. „2004“ bezeichnet das Amtsjahr 2003/04. Die errechneten Tätigkeitsanteile basieren auf der aufgewendeten Zeit in Stunden.

12.2 Beratung von Privaten und Bundesorganen

Nach Art. 28 DSG berät der EDÖB sowohl private Betroffene wie auch private Bearbeiter in Fragen des Datenschutzes. Nach Art. 31 Abs. 1 Bst. a DSG unterstützt er Organe des Bundes und der Kantone in Fragen des Datenschutzes. Er berät auch die Sachverständigenkommission

für das Berufsgeheimnis in der medizinischen Forschung (Art. 32 DSG). Die Beratung des EDÖB ist kostenlos, mit der Ausnahme von Gutachten, die der EDÖB für Private erstellt.[245]

Eingangs des Abschnitts wird der Beratungsauftrag des EDÖB kurz einem internationalen Vergleich gegenübergestellt. Im Zentrum des Abschnitts stehen danach einerseits die Gebiete und Inhalte der Beratung von Privaten und Bundesorganen durch den EDÖB, andererseits die Nützlichkeit und Praktikabilität seiner Ratschläge. Die Beantwortung der Fragen stützt sich auf Auswertungen des Geschäftsverwaltungssystems des EDÖB, auf den Tätigkeitsbericht, auf die Fallstudien zur Beratung (*SAKE, Baubranche*) sowie auf Interviews mit Bearbeitern (Private und Bund), dem EDÖB sowie weiteren Personen.

12.2.1 Beratung im internationalen Vergleich

Die im Rahmen der rechtsvergleichenden Analyse untersuchten Datenschutzbehörden übernehmen beratende Aufgaben, allerdings teilweise in unterschiedlichem Ausmass. Ein umfassendes Beratungsangebot für private und öffentliche Datenbearbeiter sowie Betroffene analog zum EDÖB kennen Frankreich, Grossbritannien, die Niederlande, Italien, Österreich sowie in Spanien. In Kanada zielt die Beratung nur auf öffentliche und private Datenbearbeiter. In Slowenien ist die Beratung zwar nicht im Gesetz vorgesehen, sie wird jedoch auch nicht ausgeschlossen. In Deutschland berät der Bundesdatenschutzbeauftragte die Bundesregierung sowie die öffentlichen Stellen des Bundes; die Beratung betroffener Personen ist nicht vorgesehen.

12.2.2 Gliederung der Beratungstätigkeit nach Sachbereichen

Die Daten des Geschäftsverwaltungssystems lassen eine Aufschlüsselung der Beratung nach Sachgebieten sowie nach der Frage zu, ob Private oder Bundesorgane beraten wurden.[246] Abbildung 12-5 zeigt den Zeitaufwand für die verschiedenen Bereiche in Stunden. Dabei schwankt die Anzahl aufgewendeter Stunden beträchtlich zwischen knapp 1500 (2007) und gegen 2500 (2010). Auch zwischen den einzelnen Tätigkeitsbereichen zeigen sich deutliche Unterschiede, die sich zudem auch im Zeitverlauf wandeln. Am meisten Aufwand leistet der EDÖB für die Beratung in den Bereichen Justiz, Polizei und Sicherheit sowie Handel und Wirtschaft. Trotz beträchtlicher Schwankungen zählen diese beiden Bereiche durchwegs zu den wichtigsten. Erst in den Jahren 2009 und 2010 sind der Gesundheitsbereich und der Bereich Statistik und Forschung wichtig geworden, während die Beratung im Arbeitsbereich an Bedeutung verloren hat. IT und Telekommunikation sowie der Versicherungsbereich verzeichnen Schwankungen ohne eindeutigen Trend nach unten oder oben.

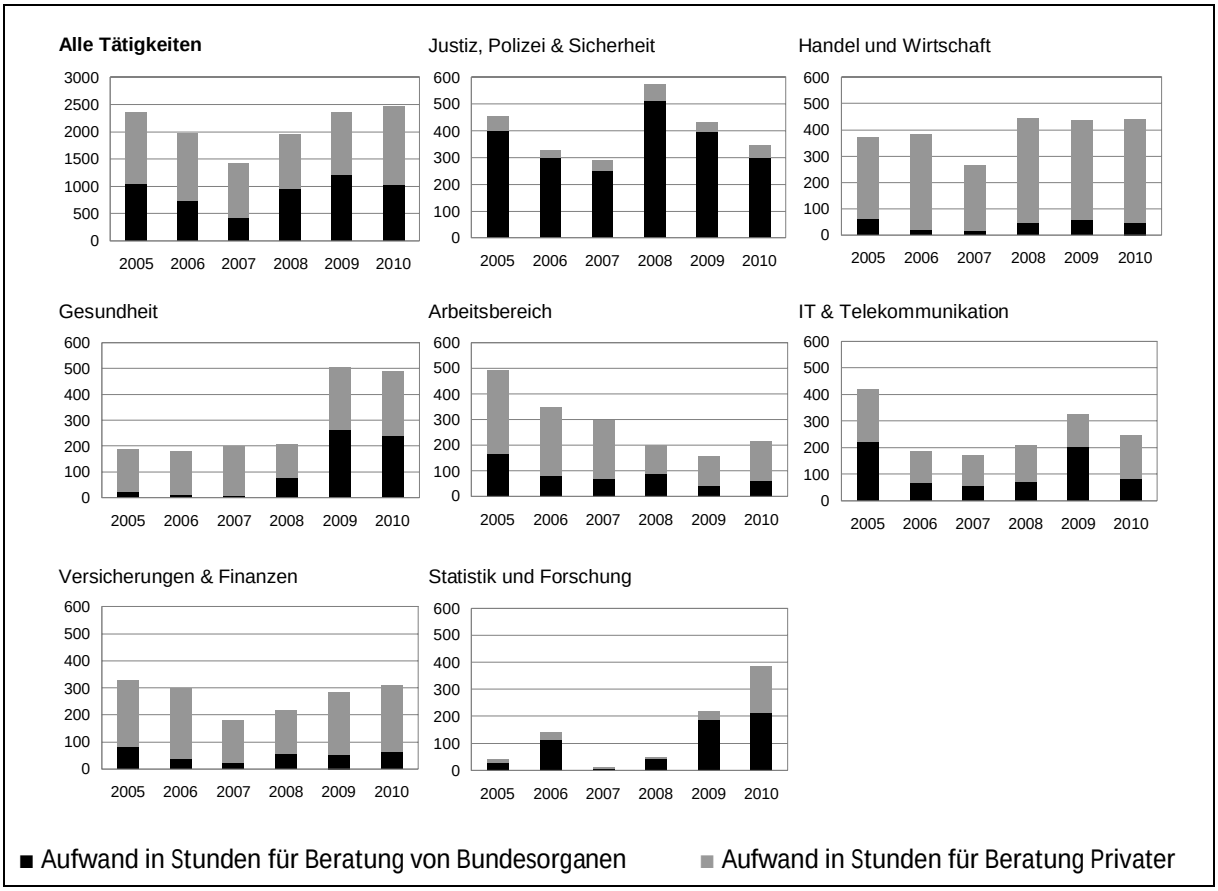
Die Beratung von Privaten nahm in allen Jahren etwas mehr als die Hälfte aller geleisteten Stunden für Beratung in Anspruch. Über alle untersuchten Jahre (2005 bis 2010) gerechnet sind es 57% Beratung von Privaten gegenüber 43% zugunsten der Bundesorgane. Eine Ausnahme bilde-

[245] Eine Gebührenpflicht für Gutachten zuhanden von Bundesorganen besteht laut Bundesverwaltungsgericht nicht. (vgl. Fall Publica: BVerwG A-5287/2008).

[246] Die Angaben im Geschäftsverwaltungssystem erlauben keine Differenzierung des Beratungsaufwands für Betroffene und Bearbeiter.

te das Jahr 2007, als der EDÖB rund 70% seiner Beratungszeit für Private aufwendete. 2008 und 2009 war der Aufwand gleichmässig auf Bundesorgane (49%) und Private (51%) verteilt. Bei der Interpretation der Statistik ist zu beachten, dass Beratungen von betroffenen natürlichen Personen auch Datenbearbeitungen von Bundesorganen zum Gegenstand haben können. Diese Differenzierung kommt in der quantitativen Auswertung nicht zum Ausdruck, so dass tendenziell der Anteil der Beratung Privater überschätzt wird. Insgesamt kann davon ausgegangen werden, dass der Zeitaufwand für die Beratung von Privaten und Bundesorganen im Vergleich zwar schwankt, aber insgesamt hinreichend ausgewogen ist.

Abbildung 12-5: Beratung von Bundesorganen und Privaten, nach Sachgebieten



Quelle: Geschäftsverwaltungssystem des EDÖB, eigene Berechnungen. Die Amtsjahre des EDÖB dauern jeweils vom 1.4. bis am 31.3. des folgenden Jahres: „2005" bezeichnet das Amtsjahr 2004/05 etc. Die errechneten Tätigkeitsanteile basieren sich auf der aufgewendeten Zeit in Stunden.

Zwischen den Sachbereichen sind bedeutende Unterschiede hinsichtlich des Zielpublikums festzustellen. Naturgemäss berät der EDÖB im Bereich Justiz, Polizei und Sicherheit überwiegend Bundesorgane; dasselbe gilt auch für Statistik und Forschung. Wenig erstaunlich ist auch, dass in Handel und Wirtschaft sowie im Versicherungs- und Finanzwesen die Beratung Privater dominant ist. Auch im Arbeitsbereich wendet der EDÖB durchgängig überwiegend Zeit für die Beratung Privater auf, was etwas weniger deutlich auch bei IT und Telekommunikation zu beobach-

ten ist, wobei 2009 eine Ausnahme bildet. Bei der Gesundheit ist das Verhältnis 2009 und 2010 ausgewogen.

Im Interview führen die befragten Mitarbeiter des EDÖB die deutlichen Schwankungen einerseits auf bewusste Planungs- und Priorisierungsentscheide, anderseits auf nicht steuerbare Entwicklungen zurück. Im Arbeitsbereich wurde gemäss den Interviewaussagen während einiger Jahre viel Zeit investiert, während nachher eine Art Sättigung eintrat und der Aufwand abnahm, auch weil Informationsmaterial nun bereitstand, das vorher erarbeitet werden musste (ein Beispiel hierfür ist der Leitfaden zur Überwachung am Arbeitsplatz). Der Justiz-, Polizei- und Sicherheitsbereich geniesst dauerhaft hohe Priorität. Der Sprung von 2008 hängt mit dem Beitritt zu den internationalen Abkommen von Schengen und Dublin zusammen. Die Zunahme im Gesundheitsbereich erklären die Verantwortlichen mit dem Thema E-health und jene bei der Statistik und Forschung hängt ihnen zufolge mit der Volkszählung (vgl. auch Fallstudie *SAKE*) zusammen. Ergänzend halten sie fest, dass viele Anfragen nicht spezifisch mit einem bestimmten Sachbereich zusammenhängen, sondern sich eher auf Aspekte des Gesetzes im Allgemeinen beziehen. Im Interview werden diesbezüglich beispielsweise Fragen zur Datensicherheit oder zur Datenbekanntgabe ins Ausland erwähnt.

12.2.3 Inhalte von Beratungen der Datenbearbeiter

Anhand der Fallstudien lässt sich die Unterschiedlichkeit der Beratungstätigkeit hinsichtlich des Umfangs der Beratungstätigkeiten aufzeigen. Im Fall *Baubranche* handelt es sich um eine kurze, einmalige Anfrage aus dem Privatbereich, die im Rahmen einer Sitzung geklärt und mit einer schriftlichen Stellungnahme abgeschlossen wurde. Im Fall *SAKE* ist die Beratung durch den EDÖB im Zusammenhang mit weiteren Aktivitäten, insbesondere mit den Arbeiten mit Blick auf die Volkszählung 2010 zu sehen und damit längerfristiger Natur. Dabei besteht ein regelmässiger Austausch (Treffen, E-Mail-Verkehr, Stellungnahmen) mit dem zuständigen Bundesamt für Statistik (BFS). Die zeitliche Beanspruchung gegenüber dem ersten Fallbeispiel ist deutlich höher.

Je nach Fall können sich auch die Zielsetzungen unterscheiden, die der EDÖB mit seiner Auswahl verfolgt: Im Fall *SAKE* sah der EDÖB in der Beratung auch die Möglichkeit, den Kontakt mit dem BFS zu intensivieren und sich nützliches Wissen anzueignen, nicht zuletzt mit Blick auf die Volkszählung 2010. Man sah in diesem Fall auch die Möglichkeit, die Bedeutung des Datenschutzes im BFS selber zu stärken. Insofern bieten Kontakte mit Bundesbehörden Möglichkeiten zur Sensibilisierung, was im Idealfall zu einer stärkeren Wahrnehmung der Aufgaben durch die Ämter oder Departemente selber und damit zu einer Entlastung des EDÖB führt.

12.2.4 Beratung von Betroffenen

Bezüglich des Aufwands haben die Beratungen von betroffenen natürlichen Personen ein grosses Gewicht; sie beziehen sich naturgemäss oft auf weniger umfassende Fragestellungen und drängen sich deshalb für eine Wiedergabe im Tätigkeitsbericht (noch) weniger auf. Rein zahlenmässig dürften die Anfragen von Betroffenen jene der Berater nach Schätzung der Interviewpartner beim EDÖB übersteigen. Genaue quantitative Aussagen können anhand des bestehenden Da-

tenmaterials nicht gemacht werden. Die Anfragen von Betroffenen betreffen nach Interviewaussagen oft den Arbeitsbereich, den Gesundheitsbereich oder das Internet. Kreditauskunfteien und der Polizeisektor im Bereich der inneren Sicherheit geben ebenfalls häufig Anlass zu Anfragen von Betroffenen.

Betroffene können sich per Post, per E-Mail (unter anderem mittels eines Kontaktformulars auf der Homepage) oder via Hotline an den EDÖB wenden. Zur Reduktion der Belastung seiner Mitarbeiter und zur Steigerung der Effizienz hat der EDÖB für telefonische Anfragen die Anrufzeiten auf der Hotline auf zwei Stunden pro Werktag beschränkt.

Einen Grossteil der schriftlichen Anfragen Betroffener bearbeitet der EDÖB anhand von Standardantworten: Wenn Betroffene eine ungerechtfertigte Verwendung ihrer Daten geltend machen oder Auskünfte von Bearbeitern möchten, so verweist sie der EDÖB in seiner Standardantwort auf ihre Möglichkeiten beim Bearbeiter und subsidiär auf den Gerichtsweg. Wenn Informationen im Internet bestehen, werden Anfrager darauf verwiesen.

Auf eine individuelle Beratung oder gar eine Intervention bei den Bearbeitern verzichtet der EDÖB in der Regel. Er verfügt jedoch über Standardbriefe, mit denen er sich bei Klagen von Betroffenen auch direkt bei bestimmten Gruppen von Bearbeitern für ein DSG-konformes Verhalten einsetzt, so bei Adressbrokern, Kreditauskunfteien und Arbeitgebern. Der EDÖB registriert und sammelt derartige Anfragen, um allfällige Häufungen, die auf gravierende Vorkommnisse deuten, nicht zu übersehen (vgl. Ziffer 12.1).

12.2.5 Die Beratung aus der Sicht der Datenbearbeiter

Ein Grossteil der im Rahmen der Interviews befragten Bearbeiter aus der Bundesverwaltung und dem Privatbereich nimmt die Beratungsleistungen des EDÖB in Anspruch. In aller Regel handelt es sich dabei um Beratung in Einzelfällen und nicht um eine häufige Kontaktierung. Der Inhalt der Beratung ist entweder eine datenschutzrelevante Frage zu einer konkreten Datenbearbeitung oder aber die (Vor-)Prüfung eines gesamten Projektes. In einem Fall (Bundesorgan) scheint ein intensiverer Austausch stattzufinden. Die Bearbeiter schätzen die Qualität der Beratung durch den EDÖB mehrheitlich als gut oder sehr gut ein: Die Ratschläge seien fundiert, nützlich und zeigten praktikable Lösungsansätze auf. Ähnliches gilt auch für die Gespräche privater Datenbearbeiter mit dem EDÖB im Rahmen des VUD. Im Rahmen der Fallstudien beurteilen die befragten Personen die Beratung als konstruktiv und kompetent.

Einzelne kritische Anmerkungen blieben aber nicht aus:

- *Wartezeiten, Nicht-Behandeln von Anfragen:* Die befragten Bearbeiter spüren im Rahmen der Beratung die Ressourcenknappheit des EDÖB. Dies äussert sich in langen Wartezeiten oder darin, dass der EDÖB nicht alle Anfragen behandeln kann. Insbesondere bei zwei Bundesämtern moniert man, dass die Beratung der Bundesorgane mit dem EDÖB zu kurz komme. Hier dürfte es zwischen den einzelnen Behörden Unterschiede geben.
- *Bundesorgane – Beratungstätigkeit schwach:* Seitens der (wenigen) befragten Datenschutzberater von Bundesorganen wird der EDÖB als wenig wahrnehmbares Beratungsorgan bezeichnet. Dies, obwohl er seinen vor einigen Jahren angekündigten Rückzug aus der Bera-

tungstätigkeit der Bundesämter teilweise rückgängig gemacht hat und ausgewählte Projekte wieder begleitet.

- *Anwendbarkeit der Beratung:* Es wurde von einer Bundesbehörde eingewendet, dass das Ergebnis der Beratung zu wenig konkret sei und damit einen geringen Nutzen stifte.
- *Verbindlichkeit:* Im Privatbereich äussert man sich verschiedentlich kritisch über die fehlende Verbindlichkeit der Beratung, weil dies die Handhabung des Investitionsrisikos erschwere. In anderen Gesprächen und in den Fallstudien hat sich gezeigt, dass in der Praxis die Meinung des EDÖB teilweise trotz ihrer rechtlichen Unverbindlichkeit faktisch als Genehmigung aufgefasst wird. Auch die Interviewpartner beim EDÖB geben an, der EDÖB sei mit dem Wunsch oder der Erwartung von Bearbeitern – seien es private oder öffentliche – konfrontiert, einer von ihm untersuchten Aktivität einen eigentlichen Stempel aufzudrücken.
- *Doppelrolle Aufsicht – Beratung:* Von privaten Datenbearbeiter wird teilweise darauf hingewiesen, dass auf Beratungen verzichtet wird, weil der EDÖB gleichzeitig als Kontrollorgan fungiere (vgl. Ziffer 12.6.1). Die Bearbeiter befürchten, aus einer Beratung könne sich eine Sachverhaltsabklärung oder eine Empfehlung ergeben, in deren Folge ihre Unternehmung eine Bearbeitung einschränken oder gar einstellen müsste. Für einen Teil der Unternehmen hat dies zur Konsequenz, dass sie sich gar nicht oder nur zu bestimmten Fragen vom EDÖB beraten lassen, nämlich in Fällen, in denen die Gefahr, dass die Datenbearbeitung eingeschränkt oder eingestellt werden muss, möglichst klein ist.
- *Wirtschaftsfreundlichkeit:* Ein Bearbeiter aus dem Privatbereich gab an, auf die Beratungsdienste des EDÖB zu verzichten und sich auf einen wirtschaftsfreundlicheren privaten Berater zu stützen.
- *Kompetenz:* Der Interviewpartner eines internationalen Konzerns befand, der EDÖB kenne die Rahmenbedingungen eines solchen Unternehmens zu wenig, als dass er nützlich beraten könne.

12.3 Aufsichtstätigkeit des EDÖB: Sachverhaltsabklärungen

Dieser Abschnitt widmet sich der Aufsichtstätigkeit des EDÖB über die Datenbearbeitungen der Bundesorgane und von Privaten. Nach einer Einführung über seine vom Gesetz vorgesehenen Aufsichtsmöglichkeiten werden diese zunächst international verglichen. Danach wird seine Aufsichtstätigkeit in der Praxis untersucht. Hinsichtlich der Entscheidungskriterien, die für die Auslösung einer Sachverhaltsabklärung herangezogen werden, kann auf Ziffer 11.2 verwiesen werden. Die Angaben stützen sich den Tätigkeitsbericht, die Fallstudien, die durchgeführten Interviews, die Dokumentation des EDÖB sowie eine Liste aller Sachverhaltsabklärungen, die 2009/10 pendent waren oder abgeschlossen wurden.

12.3.1 Rechtliche Grundlagen

Der EDÖB übernimmt Aufsichtsfunktionen über die Einhaltung des DSG sowohl bei Datenbearbeitungen durch Bundesorgane (Art. 27 DSG) als auch durch Private (Art. 29 DSG). Er kann von sich aus oder auf Hinweis von Dritten den Sachverhalt näher abklären. Bei Privaten kann er Sachverhaltsabklärungen jedoch nur durchführen, wenn mindestens eine von drei Bedingungen erfüllt ist: Die Bearbeitungsmethode muss erstens geeignet sein, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen; in diesem Zusammenhang wird von einem Systemfehler gesprochen. Zweitens klärt der EDÖB ab, wenn Datensammlungen registriert werden müssen und drittens, wenn eine Informationspflicht im Rahmen der Bekanntgabe ins Ausland besteht. Aus dem Wortlaut der Bestimmung ergibt sich nach Rosenthal und Jöhri (2008: 624), dass der EDÖB bei einem Verdacht aktiv wird und nicht Zufallsstichproben machen darf. Aus Sicht des EDÖB schliesst das DSG Zufallsstichproben nicht aus; aktuell lasse jedoch die Ressourcensituation ein solches Vorgehen nicht zu.

Im Rahmen der Abklärungen kann der EDÖB Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen, wobei für die Bearbeiter das Zeugnisverweigerungsrecht nach Art. 16 VwVG sinngemäss anwendbar ist. Die Bearbeiter sind zur Mitwirkung verpflichtet. Private Bearbeiter, die bei der Abklärung vorsätzlich falsche Auskünfte erteilen oder die Mitwirkung verweigern, können mit Busse (oder Ersatzfreiheitsstrafe) bestraft werden. Nach dem Strafgesetzbuch beträgt diese maximal 10'000 Franken. (Rosenthal/Jöhri 2008: 681).[247]

Wenn der EDÖB zum Schluss kommt, dass Datenschutzvorschriften verletzt werden, so empfiehlt er (resp. kann er empfehlen im Falle von Privaten), die Bearbeitung zu ändern oder zu unterlassen. Wird die Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit weiter ziehen. Im Falle von Bundesorganen gelangt er ans Departement, das seinen Entscheid per Verfügung den betroffenen Personen mitteilt. Der EDÖB kann gegen diese Verfügung beim Bundesverwaltungsgericht Beschwerde führen und bei einem abschlägigen Urteil ans Bundesgericht gelangen. Wenn ein Privater eine Empfehlung ablehnt oder nicht befolgt, kann der EDÖB direkt ans Bundesverwaltungsgericht gelangen und auch gegen dessen Entscheid vor Bundesgericht Beschwerde führen. Wenn der Beauftragte feststellt, dass den Betroffenen ein nicht wieder gutzumachender Nachteil droht, kann er beim zuständigen Präsidenten des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen (Art. 33 Abs 2 DSG).

Weitere Aufgaben des EDÖB mit Aufsichtscharakter sind die folgenden:

- *Rechtsetzung:* Er nimmt Stellung zu Vorlagen über Erlasse und Massnahmen des Bundes, die für den Datenschutz erheblich sind (Art. 31 Abs. 1 Bst. b DSG; vgl. hierzu Ziffer 12.7).
- *Bekanntgaben ins Ausland:* Im Zusammenhang mit den Datenbekanntgaben ins Ausland begutachtet der EDÖB das Schutzniveau der Datenschutzgesetzgebung im Ausland und prüft die Informationen im Zusammenhang mit Datenbekanntgaben ins Ausland (Art. 31 Abs. 1 Bst. d und e DSG).

[247] Bestraft werden kann ein Bearbeiter auch, wenn er seinen Informationspflichten an den EDÖB nicht nachkommt. Dies betrifft die Bekanntgabe von Daten ins Ausland nach Art. 6 DSG und die Anmeldung der Datensammlung nach Art. 11a DSG.

- *Zertifizierung:* Er ist nicht selbst für die Zertifizierung zuständig, prüft jedoch die Zertifizierungsverfahren und kann hierzu analog zur Sachverhaltsabklärung Empfehlungen abgeben (Art. 31 Abs. 1 Bst. d und e DSG).
- *Registrierung von Datensammlungen:* Der EDÖB führt das Register der Datensammlungen und macht es im Internet öffentlich zugänglich (Art. 11a DSG; vgl. Fallstudie *AVAM*, Anhang 4; Ziffer 12.3.7).
- *Medizinische Forschung:* Wenn die Sachverständigenkommission die Offenbarung des Berufsgeheimnisses bewilligt hat, so überwacht der EDÖB die Einhaltung der damit verbundenen Auflagen. Dazu kann er Abklärungen durchführen, auch kann er Kommissionsentscheide anfechten. Er wirkt auch darauf hin, dass die Patienten über ihre Rechte informiert werden.

12.3.2 Aufsichtstätigkeit im internationalen Vergleich

Tabelle 12-1 fasst wichtige Aspekte der Aufsichtstätigkeit im internationalen Vergleich zusammen. Die Tätigkeit der nationalen Aufsichtsbehörde erstreckt sich mit Ausnahme von Deutschland und teilweise Kanada sowohl auf den privat- als auch auf den öffentlich-rechtlichen Bereich und entspricht damit der Situation in der Schweiz; im Falle Deutschland wird die Aufsicht über den nicht-öffentlichen Bereich auf Länderstufe wahrgenommen.

Ein deutlicher Unterschied gegenüber der Schweiz ergibt sich hinsichtlich der Möglichkeit, Vorabkontrollen durchzuführen: Mit Ausnahme von Kanada haben alle Länder entsprechende Bestimmungen vorgesehen. In Frankreich etwa kommen je nach Art einer Datenbearbeitung unterschiedliche Formen der Vorabkontrolle zur Anwendung das österreichische Datenschutzgesetz sieht vor, dass gewisse Datenanwendungen der Vorabkontrolle durch die Aufsichtsbehörde unterliegen. Insgesamt weisen die Befunde aus dem Rechtsvergleich darauf hin, dass es sich jeweils um qualifizierte Vorabkontrollen handelt, d.h. nicht alle Datenbearbeitungen sind vorgängig der Aufsichtsbehörde zu unterbreiten, resp. je nach Datenbearbeitungen bestehen unterschiedliche Formen der Vorabkontrolle.

Tabelle 12-1 zeigt ausserdem, dass die Einwirkungsbefugnisse des EDÖB im internationalen Vergleich nicht als besonders weit reichend bewertet werden können. In einer Reihe von Ländern verfügen die Aufsichtsbehörden über die Möglichkeit, Datenbearbeitungen zu verbieten; auch die Anordnung der Sperrung, Löschung oder Vernichtung ist in einer Mehrzahl der untersuchten Staaten möglich. In Österreich und Frankreich können solche verbindliche Anordnungen teilweise nur als vorläufige Massnahme bei Dringlichkeit erlassen werden. In Deutschland, den Niederlanden und teilweise den kanadischen Provinzen verfügen die Aufsichtsbehörden demgegenüber über keine derartigen Kompetenzen; die Anordnungen sind in diesen Ländern gerichtlichen Behörden vorbehalten.

Tabelle 12-1: Aufsicht im internationalen Vergleich

	Zuständigkeit	*Vorabkontrolle*	*Einwirkungsbefugnisse*			
			Verbot Bearbeitung	*Empfehlungen*	*Gerichtsweg*	*Busse*
DE	S	ja	nein	ja	ja	ja
F	P,S	ja	ja	ja	ja	ja
GB	P,S	ja	möglich, allerdings keine spezifische Grundlage	ja	ja	ja
NL	P,S	ja	nein	ja	ja	ja
IT	P,S	ja	ja	ja	ja	ja
CND	unterschiedlich	nein	Teilweise	ja, unterschiedliche Verbindlichkeit	ja	teilweise
ÖS	P,S	ja	ja	ja	ja	nein
SL	P,S	ja	ja	ja	ja	ja
ES	P,S	ja	ja	ja	ja	ja
CH	*P,S*	*nein*	*nein*	*ja*	*ja*	*nein*

P: Aufsicht über private Bearbeiter; S: Aufsicht über staatliche Organe. Angaben ausser CH basierend auf SIR (2010).

Ein deutlicher Unterschied besteht in der Tatsache, dass eine Mehrzahl der ausländischen Behörden direkt Bussen an die Adressen der Datenbearbeiter aussprechen kann, wobei sich zwischen den verschiedenen Ländern Unterschiede bezüglich der maximalen Höhe ausmachen lassen. In Grossbritannien kann der Datenschutzbeauftragte unter ganz bestimmten Bedingungen Bussen bis zu £500‘000 aussprechen. In den Niederlanden liegen die tatsächlich ausgesprochenen Bussen zwischen 3‘000 und 15‘000 Euro. Diese Beispiele machen deutlich, dass den Geldstrafen je nach Land unterschiedliche Höchstsummen und auch unterschiedliche Voraussetzungen zu Grunde liegen.

Einer indirekten Sanktion kommen öffentlich gemachte Berichte oder Berichte an übergeordnete Stellen gleich, welche z.B. in Deutschland, Grossbritannien, in Kanada und in Italien vorgesehen sind. Besondere Sanktionsmechanismen finden sich in Deutschland und in Grossbritannien. So kann die deutsche Aufsichtsbehörde über nicht-öffentliche Datenbearbeiter die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn dieser die erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. In Grossbritannien kann die Aufsichtsbehörde beim Eingeständnis einer Rechtsverletzung auf ein Strafverfahren verzichten und eine Kaution verlangen.

Hinsichtlich der Mittel zur Informationsbeschaffung lässt sich zunächst festhalten, dass im internationalen Vergleich das Besuchsrecht (Inspektion), das Recht auf Zugang zu Daten und das Recht auf Einholung der Informationen zu den Befugnissen der Aufsichtsbehörden gezählt werden können. Das Recht auf Herausgabe ist im deutschen Recht nicht ausdrücklich geregelt (vgl. zu Deutschland allerdings die Ausführungen weiter unten in diesem Abschnitt). In Frankreich sieht das Gesetz die Herausgabe von Kopien an die Datenschutzstelle vor. Während dem EDÖB

direkt keine Zwangsmassnahmen hinsichtlich der Informationsbeschaffung zur Verfügung stehen, sehen einige Länder (Frankreich, Niederlande, Italien) diesbezüglich die Möglichkeit von direkten Bussen vor. Auch in Spanien verfügt die Datenschutzstelle in besonderen Fällen über Zwangsmöglichkeiten. Deutschland, Kanada, Grossbritannien, Österreich und Slowenien sehen dagegen wie die Schweiz keine direkten Interventionsinstrumente vor.

Schliesslich lassen sich für einzelne Staaten spezifische Instrumente aus dem Bereich der Informationsbeschaffung aufführen. In Deutschland legt das Datenschutzgesetz keine definitiven Formen für Kontrollen fest und beschränkt sich nicht auf die üblichen Informationsmittel des Auskunfts-, Akteneinsichts- und Zutrittsrechts, sondern verpflichtet die kontrollierten Stellen allgemein und umfassend zur Unterstützung. Die wichtigste Form der durchgeführten Kontrollen ist die umfassende Prüfung einer verantwortlichen Stelle durch ein Prüfteam von meist zwei bis vier Mitgliedern während eines mehrtägigen Zeitraums. Grossbritannien und Kanada kennen ausserdem die Bestimmungen, die es der Aufsichtsstelle erlauben, Personen zu befragen.

Insgesamt kann somit festgehalten werden, dass hinsichtlich der Aufsichtskompetenzen der nationalen Aufsichtsbehörde auch innerhalb Europa wesentliche Unterschiede bestehen. Dabei erweist sich die schweizerische Aufsichtsbehörde als vergleichsweise schwach ausgestattet.

12.3.3 Bedeutung der Aufsicht in den verschiedenen Sachbereichen: Überblick

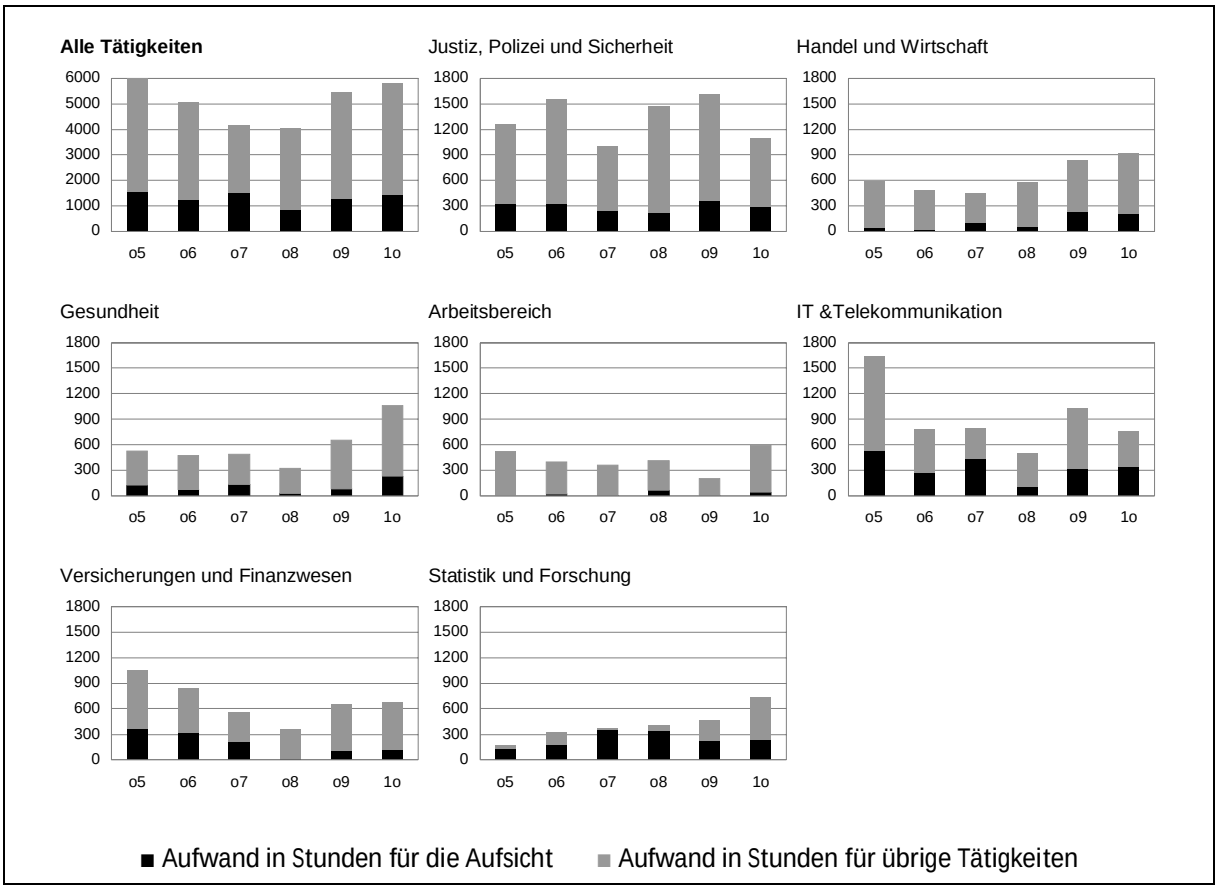
Die Zeit, welche der EDÖB für die Aufsicht aufwendet, schwankt sowohl von Sachbereich zu Sachbereich, wie auch innerhalb jedes Sachbereichs über die Zeit (Abbildung 12-6). Diese Schwankungen dürften damit zusammenhängen, dass der EDÖB mehrheitlich reaktiv handelt und somit seine Aufsichtstätigkeit nur schwer planen kann; auch erweisen sich jene Fälle, die der EDÖB vor Gericht zieht, als besonders ressourcenintensiv (vgl. Fallstudien *Logistep* und *Google Street View*).

Seit 2005 hat der EDÖB der Aufsicht in den Bereichen Justiz, Polizei und Sicherheit sowie IT und Telekommunikation am meisten Zeit gewidmet (im Durchschnitt rund 300 Stunden pro Jahr gemäss dem Geschäftsverwaltungssystem; vgl. Abbildung 12-6). Innerhalb des IT-Bereichs schwankt der Aufwand von Jahr zu Jahr stark. Im Justizbereich bleibt der Aufwand für die Aufsicht über die Zeit absolut gesehen recht konstant. Die Aufsicht hat im Vergleich zu den übrigen Aktivitäten in diesem Sachbereich einen niedrigeren Stellenwert als die Aufsicht im IT-Bereich. Bezüglich des Zeitaufwands am drittwichtigsten ist die Aufsicht bei der Statistik und Forschung, wobei dort vor allem der meist hohe relative Anteil der Aufsicht am Gesamtaufwand auffällt: Mehr als die Hälfte seiner Zeit in diesem Bereich verwendet der EDÖB für Aufsichtsprojekte. Dem Bereich Versicherung und Finanzwesen hat der EDÖB über die Jahre eher abnehmend Aufmerksamkeit gewidmet. Eine eher kleine Rolle spielen das Gesundheitswesen, Handel und Wirtschaft (mit Ausnahme von 2009 und 2010) sowie der Arbeitsbereich.

Eine Aufteilung des Aufwands für die Aufsicht zwischen Bund und privaten Datenbearbeitern ist anhand der Daten des Geschäftsverwaltungssystems des EDÖB nicht möglich. Eine Übersicht über sämtliche Sachverhaltsabklärungen (sowie ihre Resultate und Wirkungen) besteht beim EDÖB nicht. Eine vom EDÖB für die Evaluation zusammengestellte vollständige Liste der

Sachverhaltsabklärungen, die im Amtsjahr 2009/10 abgeschlossen wurden oder an dessen Ende noch hängig waren, enthält 49 Projekte; davon sind 25 jener Einheit des EDÖB zuzuordnen, die sich überwiegend mit den Datenbearbeitungen von Behörden oder von Privaten in behördlicher Funktion (z.B. Krankenversicherungen im Bereich der Grundversorgung) auseinandersetzt (Quelle: EDÖB). Eine Minderheit dieser Projekte betrifft zwar auch private Datenbearbeitungen. Dennoch kann davon ausgegangen werden, dass die vom EDÖB angestrebte Ausgewogenheit der Aufsicht über Behörden und Private in der jüngsten Vergangenheit etwa erreicht worden ist.

Abbildung 12-6: Aufsicht und übrige Aktivitäten des EDÖB, nach Sachgebieten



Quelle: Geschäftsverwaltungssystem des EDÖB, eigene Berechnungen. Die Amtsjahre des EDÖB dauern jeweils vom 1.4. bis am 31.3. des folgenden Jahres: „2005" bezeichnet das Amtsjahr 2004/05 etc. Die errechneten Tätigkeitsanteile basieren auf der aufgewendeten Zeit in Stunden.

Die Auswertung der Tätigkeitsberichte erlaubt weitere Aufschlüsse über die Sachgebiete und die konkreten Inhalte der Sachverhaltsabklärungen. In den Tätigkeitsberichten von 2001/02 bis 2009/10 wurden durch die Autoren der Evaluation 94 von rund 500 Aktivitäten als Sachverhaltsabklärungen eingestuft. Deren 39 (41%) betrafen Aktivitäten des EDÖB im Rahmen seiner Aufsichttätigkeit über Bundesorgane (Art. 27 DSG) und die medizinische Forschung (Art. 32 DSG), die übrigen 55 Abklärungen befassten sich mit Datenbearbeitungen von Privaten (Art. 29 DSG). Auch in den Tätigkeitsberichten ergibt sich somit der Eindruck eines in etwa ausgewogenen Verhältnisses zwischen der Beaufsichtigung von Bundesorganen und Privaten. Es zeigen sich dabei

Unterschiede zwischen dem privaten und dem öffentlich-rechtlichen Bereich: Im Privatbereich liegen die zahlenmässigen Schwerpunkte von publizierten Sachverhaltsabklärungen in den Bereichen Allgemein und Grundrechte, Handel und Wirtschaft sowie Arbeit; hinsichtlich der Bundesorgane liegen die Schwerpunkte in den Bereichen Versicherungen sowie Justiz, Polizei und Sicherheit; ebenfalls häufig sind Abklärungen in den Gebieten Statistik und Forschung.

Diese Verteilung entspricht nicht durchwegs dem Bild, das sich oben bei der Erfassung des Zeitaufwands für die Aufsicht ergeben hatte. Die Abweichung kann hier nicht vollständig aufgeklärt werden. Sie könnte zum einen daher rühren, dass beispielsweise im zahlenmässig stark vertretenen Arbeitsbereich recht viele kleinere Abklärungen durchgeführt werden und beispielweise im IT- und Telekommunikations-Bereich eher wenige, dafür aufwändige. Der Unterschied könnte prinzipiell aber auch daran liegen, dass der Tätigkeitsbericht nur selektiv informiert und bei der Berichterstattung auch andere Gewichtungsfaktoren (thematische Ausgewogenheit) eine Rolle spielen. Dass der Arbeitsbereich im Tätigkeitsbereich ein derart grosses Gewicht erhält, ist gleichwohl überraschend. Die Interviewpartner beim EDÖB bezeichnen den Arbeitsbereich als vergleichsweise sensibel, da die Betroffenen sich in einem Subordinationsverhältnis befinden. Dieses Kriterium ist beim EDÖB für die Durchführung von Sachverhaltsabklärungen wichtig.

12.3.4 Auslösung von Sachverhaltsabklärungen

Beim Entscheid über die Durchführung einer konkreten Abklärung versucht sich der EDÖB auch an den Tätigkeitsschwerpunkten zu orientieren, die er sich im Rahmen der Jahresplanung selbst vorgibt (Interviewaussage). Ob eine Sachverhaltsabklärung durchgeführt wird, entscheidet der EDÖB im Rahmen des in Ziffer 11.2.3 beschriebenen Triage-Prozesses, den alle eingehenden Hinweise durchlaufen, und der sich angelehnt an die Vorgaben des DSG am Risikopotenzial eines Falls orientiert.

Meist steht eine Information durch eine oder mehrere Personen oder Organisationen ausserhalb der Behörde am Anfang von Sachverhaltsabklärungen. Solche Hinweise kommen von Betroffenen, von anderen Behörden (vor allem von der Finanzkontrolle, teils von den parlamentarischen Geschäftsprüfungskommissionen, selten von anderen Behörden) oder auch von den Medien, gelegentlich auch von Mitarbeitern des Datenbearbeiters. Auch im Rahmen der internationalen Zusammenarbeit können sich Hinweise für Sachverhaltsabklärungen ergeben (vgl. zur Auslösung der Abklärungen auch Tabelle 11-2). Einzelne Beschwerden von betroffenen Personen sind wie gezeigt noch kein Grund für den EDÖB, eine Sachverhaltsabklärung auszulösen. Solche Hinweise werden jedoch klassifiziert und gespeichert, sodass der EDÖB eine Häufung von einzelnen Beschwerden zu einem bestimmten Bearbeiter (oder einem bestimmten Typ von Bearbeitungen) feststellen kann (vgl. Ziffer 11.2.3). Eine solche Häufung kann schliesslich zu einer Sachverhaltsabklärung führen.

Mit dieser Praxis legt der EDÖB in der Wahrnehmung der juristischen Literatur die Voraussetzungen, die für die Durchführung einer Sachverhaltsabklärung (bei privaten Bearbeitern) gegeben sein müssen, eher weit aus. Während der Wirkungsmechanismus der Durchsetzungsrechte auf dem Gerichtsweg auf Einzelfälle ausgelegt ist, sollten die Sachverhaltsabklärungen des EDÖB dann einsetzen, „wenn eine unrechtmässige Datenbearbeitung eine grössere Anzahl Betroffener

zur Folge hat“ (Huber 2006: 394; vgl. auch Bundesrat/BBl 1988 II 479). Dabei stellt sich die Frage, ob diese Voraussetzung nur dann gegeben ist, wenn wegen der Bearbeitung eines *einzelnen* Bearbeiters eine grössere Anzahl Personen betroffen ist, oder auch dann, wenn sich eine grössere Anzahl Betroffener nur dadurch ergibt, weil *mehrere* Bearbeiter Daten *gleichartig* bearbeiten. Der EDÖB hat die Voraussetzung in seiner Praxis in beiden Konstellationen als erfüllt betrachtet (Huber 2006: 395). Rosenthal/Jöhri (2008: 625) kommen ebenfalls zum Schluss, der ursprünglichen Idee, über Art. 29 DSG nur jene Fälle abzudecken, die sich wegen der Vielzahl betroffener Personen über die Zivilgerichte nicht mehr angemessen behandeln lassen würden, werde „heute nicht mehr strikte nachgelebt“. Den beiden Autoren zufolge ist jedoch der Spielraum des EDÖB zur Auslösung einer Sachverhaltsabklärung gross. Als Mindesterfordernis erwähnen sie, dass ein konkreter Verdacht bestehen muss, und somit eine Abklärung nicht im Sinne einer Zufallsstichprobe durchgeführt werden darf (Rosenthal/Jöhri 2008: 624).

In den Fallstudien privater Datenbearbeitungen ist das gesetzlich verlangte Verdachtsmoment für die Durchführung der Abklärung überall zweifelsfrei gegeben. *Google Street View* ist potenziell sicher geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen, gleiches gilt auch für die Fälle *Logistep* und *Mitarbeitercheck*.

In den Fallstudien ist im Weiteren deutlich geworden, dass nicht immer Dritte Sachverhaltsabklärungen auslösen. Es kommt auch vor, dass sich aus laufenden anderweitigen Projekten des EDÖB Sachverhaltsabklärungen ergeben. Die Beratung im Fall *SAKE* veranlasste den EDÖB dazu, anschliessend zwei Fragestellungen im Rahmen seiner Aufsichtstätigkeit zu untersuchen. Auch im Fall *Krankenversicherer* beabsichtigt der EDÖB, im Anschluss an die gemachte Erhebung zur datenschutzrechtlichen Situation gezielt weitere Abklärungen durchzuführen. Auslöser der Umfrage war nicht zuletzt eine bei einer Krankenversicherung durchgeführte Abklärung, welche deutliche Datenschutzmängel ergeben hatte. Grundsätzlich weist der EDÖB auch im Rahmen seiner Beratungstätigkeit auf seine Rolle als Aufsichtsorgan hin.

12.3.5 Sachverhaltsabklärungen im Bereich neuer Konstellationen

Die Fälle, über die der EDÖB im Tätigkeitsbericht berichtet, hinterlassen den Eindruck, dass so genannte klassische Konstellationen im Bereich der Sachverhaltsabklärungen dominieren. Dies ist systemimmanent: Abklärungen können nur dort stattfinden, wo der EDÖB auf den Bearbeiter zugreifen kann, was voraussetzt, dass dieser klar identifizierbar ist und praktischerweise seinen Sitz in der Schweiz hat. Es gibt zwar Internet-Anwendungen, bei denen dies der Fall ist und bei denen der EDÖB auch eingegriffen hat (vgl. z.B. den Fall *Mitarbeiter-Check).* Diese Fälle sind aber insofern klassisch, als die Bearbeiter für die Betroffenen und den EDÖB eindeutig identifizierbar sind und in der Schweiz operieren. Doch ist bei Internetanwendungen anzunehmen, dass die Betroffenen von Verletzungen der Datenschutzgrundsätze, die im Internet geschehen, oftmals gar keine Kenntnis haben, oder möglicherweise in problematische Bearbeitungen eingewilligt haben, in dem sie entsprechende Vertragsbedingungen angekreuzt haben. In beiden Fällen sehen sie sich nicht veranlasst, den EDÖB zu kontaktieren, womit diese Informationsquelle für ihn in diesen Konstellationen versiegt ist.

Diese Grenzen der Sachverhaltsabklärung als Instrument zur Durchsetzung des Datenschutzgesetzes in diesen neuen Konstellationen lassen sich auch an den Fallstudien veranschaulichen: Im Fall *Logistep* und im Fall *Google Street View* waren es nicht die Betroffenen, die eine Abklärung auslösten, sondern einmal andere Datenschutzbehörden aus dem Ausland, und einmal die breite öffentliche Diskussion. Aufschlussreich bezüglich der Auswahl von Sachverhaltsabklärungen ist vor allem ein Blick auf zwei Fälle aus dem Bereich neuer Technologien, in denen der EDÖB (bisher) auf keine Sachverhaltsabklärung durchgeführt, sondern nur informiert hat. So hat der EDÖB bisher im Bereich des *Mobile Computing*, das durchaus datenschutzrechtliche Risiken birgt, auf eine Abklärung verzichtet, weil entsprechende Verdachtsmeldungen bisher nicht eingetroffen seien. Auch zu *Sozialen Netzwerken* hat der EDÖB zwar eine Stellungnahme und Tipps für Anwender, Bearbeiter und Schulen veröffentlicht, aber keine Abklärung durchgeführt. Neben der Tatsache, dass die Dateneingabe hier bewusst erfolgt und somit dem Betroffenen auch eine Eigenverantwortung und Massnahmen des Selbstschutzes zugemutet werden kann, spielten hier auch taktische Überlegungen des EDÖB eine Rolle. Er erachtete die Erfolgsaussichten einer Abklärung bei einem Grossunternehmen wie Facebook, das im Unterschied zu Google keinen Sitz in der Schweiz hat, als gering.

12.3.6 Durchführung von Sachverhaltsabklärungen: Informationsbeschaffung

Aufgrund dieser beschränkten Mittel der Informationsbeschaffung (vgl. Ziffer 12.3.2) ist der EDÖB bei seinen Abklärungen auf die Zusammenarbeit mit den Datenbearbeitern angewiesen. Er meldet seine Kontrollen nicht zuletzt aus diesem Grund praktisch immer an und erläutert den Datenbearbeitern seine rechtlichen Möglichkeiten sowie ihr Risiko einer Anzeige, falls sie nicht kooperieren. Gemäss den gemachten Interviewaussagen ist es die Strategie des EDÖB, den Bearbeitern vor Augen zu führen, dass sie ein Interesse an einer korrekt durchgeführten Abklärung und korrekten Datenbearbeitungen haben.

Bezüglich der Zusammenarbeit stellten die befragten EDÖB-Vertreter Unterschiede zwischen Privaten und Bundesorganen fest:

- *Privatsektor:* Im Privatsektor ist die Bereitschaft zur Zusammenarbeit während der Kontrolle normalerweise gut und die Bereitschaft zur Herausgabe der Informationen vorhanden. Die EDÖB-Mitarbeiter kamen im Interview zum Schluss, die Privatunternehmer merkten jeweils schnell, dass sie aus Marketinggründen (vgl. Imagerisiko) an einem guten Zeugnis des EDÖB interessiert seien. Hinweise hierzu ergaben sich teils auch in den Fallstudien, so insbesondere im Fall *Krankenversicherung*. Allerdings bestünden innerhalb der Unternehmenswelt Unterschiede bezüglich der Kooperationsbereitschaft und der Sensibilität für Datenschutzfragen. In der Regel stosse der EDÖB bei Grossunternehmen, die über eigene Strukturen im Bereich Datenschutz verfügten, auf mehr Verständnis. In den Fallstudien fanden sich Beispiele, in denen die Kooperationsbereitschaft der Datenbearbeiter und die Möglichkeiten zur Informationsbeschaffung durch den EDÖB kritisch beurteilt wurde: So war es im Fall *Google Street View* bislang für den EDÖB nicht möglich, die eingesetzte Anonymisierungssoftware näher zu untersuchen (vgl. Klageschrift des EDÖB); stattdessen musste er sich zu einem grossen Teil auf die Angaben des Datenbearbeiters stützen. Auch zeigte sich

in den Fallstudien, dass es für den EDÖB teilweise schwierig ist zu beurteilen, inwiefern die Datenbearbeiter tatsächlich die relevanten Informationen bereitstellen. Hier bestehen gewisse Möglichkeiten, den Informationsfluss an den EDÖB zu steuern, was für diesen nur schwer nachzuweisen ist.

- Bei den *Bundesorganen* ist nach den Interviewaussagen die Furcht der Bearbeiter, Informationen herauszugeben, präsenter und der Erklärungsaufwand für den EDÖB – etwa über seine Rechte, aber auch über die Interessen der Bearbeiter an einer einwandfreien Datenbearbeitung – höher. Meist werde dann jedoch schon kollaboriert, wobei gelegentlich die Kontrolle über den Amtsleiter eingefädelt werden müsse. Die Befragten berichten auch von Fällen, in denen man dem EDÖB Informationen vorenthalten wollte mit der Begründung, sie seien für die Abklärung nicht relevant. Bei den Bundesorganen ist somit der Aufwand, um an die Informationen zu gelangen, grösser. Die Interviewpartner gaben aber an, in der Regel zum Ziel zu kommen. Auch unter den Bundesorganen beobachten die Interviewpartner beträchtliche Unterschiede.

In den Fallstudien hat sich darüber hinaus gezeigt, dass der EDÖB nicht immer gänzlich auf die Mitwirkung des Bearbeiters angewiesen ist. So beschrieb das Unternehmen im Fall *Mitarbeitercheck* die Datenbearbeitung in ihrem Werbe-Mail an Personalverantwortliche so ausführlich, dass der EDÖB bereits aufgrund dieser Informationen in der Lage war, eine (später durch das Bundesverwaltungsgericht gutgeheissene) provisorische Massnahme zu beantragen. Im Fall *Google Street View* waren Bilder, in denen die Anonymisierungssoftware des Anbieters nicht funktioniert hat, auf dem Internet frei zugänglich. Andere Aspekte jedoch wie die Archivierung des Bildmaterials waren für den EDÖB nicht einfach einsehbar.

Obwohl der EDÖB in der Regel nach der Einschätzung der befragten Mitarbeitenden die relevanten Informationen erhält, wünschten sich die Interviewpartner zur Steigerung ihrer Effektivität und Effizienz weitergehende Informationsmittel, so etwa auch die Möglichkeit, Informationen beschlagnahmen zu können oder in gewissen Fällen Systemzugang zu erhalten. Sie begründen dies mit der technologischen Entwicklung, welche es zunehmend erschwere, mit den bisherigen Mitteln einen genügenden Einblick in Datenbearbeitungen zu erhalten.

12.3.7 Register der Datensammlungen und Kontrolle von Bearbeitungsreglementen

Im Bereich der Aufsichtstätigkeit des EDÖB stellt die Kontrolle von Bearbeitungsreglementen einen Spezialfall dar. Sie bezieht sich auf Datensammlungen, die im öffentlichen Register des Beauftragten nach Art. 11a DSG angemeldet sind. Dieser Bestimmung zufolge müssen die Bundesorgane sämtliche Datensammlungen anmelden. Private müssen Sammlungen nur anmelden, wenn regelmässig besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden oder wenn regelmässig Personendaten an Dritte bekannt gegeben werden. Das Register soll einerseits den Betroffenen Hinweise über mögliche Datensammlungen von ihnen bieten, andererseits dem EDÖB einen Überblick über die bestehenden Datensammlungen verschaffen. Wenn er in einer registrierten Datensammlung einen Verstoss erblickt, kann er eine Sachverhaltsabklärung durchführen. Gemäss der Standardliteratur ist das allerdings bislang praktisch nie vorgekommen (Belser 2006: 170). Für Datensammlungen mit bestimmten Eigenschaften besteht darüber hinaus

die Pflicht, ein Bearbeitungsreglement zu erarbeiten (Art. 11 VDSG für Private, Art. 21 VDSG für Bundesorgane). Dieses gibt Auskunft über die interne Organisation der betreffenden Datenbearbeitung sowie über das Datenbearbeitungs- und Kontrollverfahren und enthält die Unterlagen über die Planung, Realisierung und den Betrieb der einzelnen Datensammlung und der zugehörigen Informatikmittel (vgl. auch EDSB 1994; EDÖB 2009).

Umsetzung der Vorschrift zur Registrierung

Der EDÖB führt das Register, hat aber keine Kontrolle darüber, ob tatsächlich alle Bearbeiter ihre registrierpflichtigen Datensammlungen angeben und ein Bearbeitungsreglement erstellen, wo dies verlangt ist. Bei den Bundesorganen besteht eine gewisse Übersicht dadurch, dass für Datensammlungen eine gesetzliche Grundlage bestehen muss, über die der EDÖB aufgrund seiner Aufgaben im Bereich der Rechtsetzung (Art. 31 Abs. 1 Bst. b) gut informiert ist (vgl. Ziffer 12.7). Bei den Privaten ist er auf die Redlichkeit der Bearbeiter und auf Hinweise von Betroffenen angewiesen. Wie gut der Registrierpflicht tatsächlich nachgelebt wird, kann nicht abschliessend beurteilt werden. Mit Lücken ist jedoch zu rechnen. Einen deutlichen Hinweis hierauf ergab für den Gesundheitsbereich die gemeinsame Umfrage des BAG und des EDÖB zu Datenschutzfragen (Fall *Krankenversicherer*). Von 93 anerkannten öffentlichen Krankenversicherern verfügten nur 26% (mit 62% der Versicherten) über ein Bearbeitungsreglement (BAG/EDÖB 2009: 39-40). 27% der Versicherer legten ihrem ausgefüllten Fragebogen ein Dokument bei, das kein Bearbeitungsreglement ist. Auch ein Interviewpartner äusserte sich äussert skeptisch zur Bereitschaft, sich ins Register einzutragen, aber auch zur Nutzung durch die Betroffenen. Er bezeichnet das Register als Formalie, die den Bearbeitern das Leben schwer mache, ohne dem Datenschutz effektiv etwas zu bringen. Die befragten Personen beim EDÖB hingegen sehen im Register durchaus einen Nutzen (Transparenzgewinn für die Betroffenen und den EDÖB). Im internationalen Vergleich zeigt sich, dass die meisten Länder über ein Register verfügen, wobei der Eintrag teils mit einer Vorabkontrolle der Bearbeitung verbunden sein dürfte. In Grossbritannien z.B. ist die (gebührenpflichtige) Registrierung gleichbedeutend mit der Erteilung einer Bearbeitungsbewilligung (Belser 2006: 179).

Umsetzungskontrolle und Wirkung von Bearbeitungsreglementen

Der Zweck des Bearbeitungsreglements ist es, den Bearbeiter zum Erstellen eines eigentlichen Handbuchs über seine Datensammlung zu bewegen und so für Transparenz über seine Bearbeitung nach innen und aussen zu sorgen. Gemäss dem Kommentar zur VDSG liegt ein solches Reglement „sowohl im Hinblick auf den Datenschutz als auch auf eine rationelle Betriebsführung im Interesse jedes Verantwortlichen einer automatisierten Bearbeitung“ (Kommentar 2008: Ziffer 6.2.2) Soll es gegen innen somit die Organisation dazu bringen, sich Rechenschaft über die datenschutzsensitiven Prozesse geben und diese korrekt zu organisieren, sorgt es gegen aussen für Transparenz. Gemäss Aussagen der EDÖB-Mitarbeitenden dient das Reglement denn auch stark der Sensibilisierung der zuständigen Personen einer Organisation. Auch der befragte Bearbeiter der Fallstudie *AVAM* gab zu Protokoll, das Bearbeitungsreglement sei geeignet, um für die entsprechende Datensammlung Transparenz herzustellen und sich selber Rechenschaft über die

Datenbearbeitungen abzulegen. Eine generelle Sensibilisierung über die konkrete Anwendung hinaus sei jedoch nicht zu erwarten.

Wie erwähnt hat der EDÖB nicht den vollständigen Überblick über jene Datensammlungen, die ein Bearbeitungsreglement erfordern, kennt aber im Bereich der Bundesverwaltung nach seinen Aussagen die laufenden Projekte, welche potenziell besonders schützenswerte Daten oder Persönlichkeitsprofile enthalten, relativ gut. Nach Aussagen seiner Mitarbeiter fordert er jährlich rund zehn Reglemente zur Durchsicht an, von denen er deren drei bis vier einer vertieften Untersuchung unterzieht. Wenn die Kontrolle sich auf die Einhaltung der formellen Anforderungen eines Bearbeitungsreglements (vgl. auch EDÖB 1994; EDÖB 2009) beschränkt, ist sie nicht sonderlich aufwändig. Gleichzeitig bietet ein korrektes Reglement keine Gewähr für eine auch tatsächlich korrekte Datenbearbeitung. Wenn der EDÖB tiefer schürft oder an die Kontrolle eine tatsächliche Sachverhaltsabklärung anschliesst, steigt der Aufwand hingegen deutlich an. Dies kommt jedoch selten vor. Der Prozess von der Anforderung des Reglements bis zur bereinigten Version des Reglements kann sich dennoch über einen längeren Zeitraum hinziehen, bei Anpassungen der Bearbeitung ist zudem auch das Reglement zu aktualisieren. Bei der Fallstudie *AVAM* fand die erste Kontrolle im Amtsjahr 2006/2007 statt, der letzte den Evaluatoren vorgelegte Briefwechsel datiert vom Herbst 2009.

Trotzdem bezeichnen die Befragten beim EDÖB die Kontrolle von Reglementen als relativ effizientes und notwendiges Instrument, wie auch aus dem Tätigkeitsbericht hervorgeht: „Bei den von uns kontrollierten Bearbeitungsreglementen sind in vielen Fällen noch Mängel in der Umsetzung der technischen und organisatorischen Massnahmen festzustellen“ (EDÖB 2006/07: 33). Auch im Tätigkeitsbericht 2008/09 wird festgestellt, dass „Bearbeitungsreglemente in vielen Fällen nicht entsprechend den Vorgaben geführt werden“ (EDÖB 2008/09: 32).

Zusammenfassend kann festgehalten werden, dass die Bearbeitungsreglemente prinzipiell wohl ein wirksames Sensibilisierungsinstrument für Fragen des Datenschutzes bei den Datenbearbeitern sind. Aufgrund der vorliegenden Hinweise des EDÖB muss jedoch vermutet werden, dass der Verpflichtung zur Führung eines Bearbeitungsreglements teils nur widerwillig und ungenügend nachgelebt wird. Teilweise werden sowohl die Registrierpflicht als auch das Bearbeitungsreglement, so ist gemäss Interviewaussagen zu vermuten, als unnötige bürokratische Hürde empfunden. Der EDÖB seinerseits hat insbesondere im Privatbereich weder die Übersicht noch die Mittel, sicherzustellen, dass die gesetzlichen Vorschriften der Registrierung und der Bearbeitungsreglemente von den Bearbeitern eingehalten werden. An der Wirksamkeit dieser Vorschriften in der Breite bestehen somit erhebliche Zweifel.

12.4 Resultate und Wirkungen von Sachverhaltsabklärungen

Dieser Abschnitt widmet sich den Resultaten der Sachverhaltsabklärungen. Es geht dabei um die Frage, wie oft der EDÖB bei seinen Sachverhaltsabklärungen Grund zu Beanstandungen findet und den Bearbeitern Massnahmen nahe legt. Wir unterscheiden dabei zwischen Verbesserungsvorschlägen, welche sich auf eher kleine Massnahmen beziehen, und Empfehlungen im Sinne von Art. 27 und 29 DSG. Schwerpunkte des Abschnitts bilden die Umsetzung der Empfehlungen durch die Bearbeiter und deren Durchsetzung vor höherer Instanz. Ergänzend wird auch die

Frage beleuchtet, inwieweit der EDÖB sicherstellen kann, dass seine Sachverhaltsabklärungen Wirkungen über den einzelnen Fall hinaus erzielen können. Da hierzu beim EDÖB bisher keine umfassenden Daten vorliegen, stützen sich die Ausführungen auf die Tätigkeitsberichte und die im Internet publizierten Empfehlungen ab. Auch die Fallstudien dienten als Grundlage für die Analyse.

12.4.1 Verbesserungsmassnahmen und Empfehlungen

Der EDÖB unterscheidet bei seinen Sachverhaltsabklärungen zwischen zwei Stufen von Handlungsanweisungen. Neben der gesetzlich vorgesehenen Empfehlung, gegen deren Nichtbefolgung er bei höherer Instanz intervenieren kann, gibt es auch die so genannten Verbesserungsmassnahmen.

- *Empfehlungen* spricht der EDÖB immer dann aus, wenn er eine klare Verletzung des DSG feststellt, die er nach seiner Einschätzung im Konfliktfall auch vor Gericht erfolgreich durchsetzen könnte. Die Praxis des EDÖB ist es, konsequent vor Gericht zu gehen, wenn ein Bearbeiter seine Empfehlung nicht umsetzt. Die Interviewpartner vertraten die Auffassung, ein anderes Vorgehen schade der Glaubwürdigkeit des EDÖB. Festgehalten sei hier, dass der EDÖB die Empfehlung als seine härteste Sanktionsmöglichkeit als unzureichend bezeichnet. Er fordert, in bestimmten Situationen als ultima Ratio die Bearbeitung unter Androhung einer Administrativmassnahme oder -busse direkt unterbinden zu können. Schon heute kann der EDÖB beim Bundesverwaltungsgericht eine provisorische Massnahme beantragen, welche eine Datenbearbeitung temporär unterbinden kann, bis der Sachverhalt abgeklärt ist (vgl. die Fälle *Mitarbeitercheck* und *Google Street View*). Empfehlungen werden in der Regel veröffentlicht, wenn auch teils anonymisiert. Bisweilen ist nach Einschätzung der Interviewpartner der durch die Veröffentlichungsdrohung entstehende Druck für die Bearbeiter fast stärker als der Druck, der von einer möglichen Sanktion ausgeht.
- *Verbesserungsmassnahmen:* Wenn der EDÖB auf Probleme stösst, bei denen ein Interpretationsspielraum besteht oder die nicht so gravierend erscheinen, legt er dem Bearbeiter Verbesserungsmassnahmen nahe, wobei er ihm diesbezüglich durchaus auch beratend zur Seite steht (vgl. Fallstudie *AVAM*). Wie die Interviewpartner beim EDÖB versichern, können auf diesem Weg bisweilen Blockaden und Machtproben vermieden werden und für den Datenschutz mehr erreicht werden.

Die vom EDÖB beanstandeten Mängel verstossen sowohl bei den Bearbeitungen von Privaten als auch von Bundesorganen nur in einer Minderheit der Fälle so offensichtlich gegen das DSG, dass dieser sich zu einer oder mehreren Empfehlungen veranlasst sieht.[248] In diesen Befunden widerspiegelt sich, dass der EDÖB auch im Rahmen seiner Aufsichtstätigkeit einen durchaus pragmatischen Ansatz verfolgt und darum bemüht ist, einvernehmliche und praktikable Lösun-

[248] Quantitative Aussagen lassen sich aufgrund fehlender Daten nur sehr beschränkt machen. Für die in den Tätigkeitsberichten publizierten Sachverhaltsabklärungen liegt die Quote der Abklärungen, die zu einer Empfehlung führen, bei 22%. Dieser Wert dürfte den tatsächlichen jedoch überschätzen, weil im Tätigkeitsbericht vermutlich überproportional viele Fälle mit Problemen erwähnt werden.

gen mit den Datenbearbeitern zu finden. Dabei wird in den seltensten Fällen die Einstellung der Datenbearbeitung gefordert, sondern aufgezeigt, welche organisatorischen oder technischen Massnahmen ergriffen werden können, um eine Bearbeitung datenschutzkonform zu gestalten.

Ein anderes Bild ergibt sich in denjenigen Fällen, in denen es zu einer Empfehlung kommt: Die inhaltliche Auswertung der Empfehlungen haben ergeben, dass in rund der Hälfte der Empfehlungen vom EDÖB eine partielle oder vollständige Einstellung der Datenbearbeitung gefordert wird.

12.4.2 Umsetzung und Durchsetzung von Empfehlungen

Tabelle 12-2 vermittelt einen Überblick über die Umsetzung der 23 im Internet und den Tätigkeitsberichten seit 2001 veröffentlichten Empfehlungen. Die Zahlen zeigen, dass sich die Datenbearbeiter gegen einen substanziellen Anteil der Empfehlungen sträuben: In rund der Hälfte aller Fälle setzen sie die Empfehlungen des EDÖB nicht oder nicht vollständig um. Aufgrund der vorliegenden Auswertung lassen sich bezüglich der Umsetzungswahrscheinlichkeit keine substanziellen Unterschiede zwischen dem öffentlich-rechtlichen und dem privaten Bereich feststellen.

Tabelle 12-2: Umsetzung der Empfehlungen durch die Datenbearbeiter

	Privat	*Bund*	*Total*
Direkte Umsetzung	9	2	11
Keine direkte Umsetzung	9	3	12
Total Empfehlungen	*18*	*5*	*23*

Quelle: Publizierte Empfehlungen des EDÖB 2001 bis 2010. Tätigkeitsberichte; Homepage EDÖB; schriftliche Auskünfte des EDÖB.

In denjenigen Fällen, in denen die Datenbearbeiter den Empfehlungen nicht nachgekommen sind, hat der EDÖB (bis auf eine spezifische Ausnahme aus dem Privatbereich[249]) immer versucht, seine Empfehlung auf dem Rechtsweg durchzusetzen.[250] Acht Weiterzüge betrafen den Privatbereich und gingen an die EDSK resp. EDÖK (bis 2006) oder an das Bundesverwaltungsgericht; die drei Empfehlungen aus der Aufsichtstätigkeit über Bundesorgane mussten vom zuständigen Departement beurteilt werden. Somit kommt der oben beschriebene Automatismus auch in den Daten zum Ausdruck: Hat sich der EDÖB einmal entschieden, eine Empfehlung zu erlassen, zieht er bei einer Nicht-Berücksichtigung durch den Datenbearbeiter den Fall weiter.

[249] Dabei handelt es sich um den Fall „Recommandation à propos d'une caméra de surveillance installée dans le Chalet SJ" vom 18. Februar 2009, in der sich der EDÖB mit Hilfe der französischen Datenschutzbehörde schliesslich durchsetzen konnte.

[250] Rosenthal und Jöhri kommen für den Privatbereich zu einem etwas anderen Schluss: „In der bisherigen Praxis wurden abgelehnte oder nicht befolgte Empfehlungen zwar meistens, aber nicht immer der gerichtlichen Beurteilung (…) vorgelegt" (Rosenthal/Jöhri 2008: 635). Als Gründe für den Verzicht nennen die Autoren, dass die Adressaten der Empfehlung ihre Haltung begründen können oder neue Erkenntnisse vorliegen. Huber (2006: 400) weist darauf hin, dass im Zusammenhang mit Empfehlungen zum Teil Stillschweigen gewahrt wird.

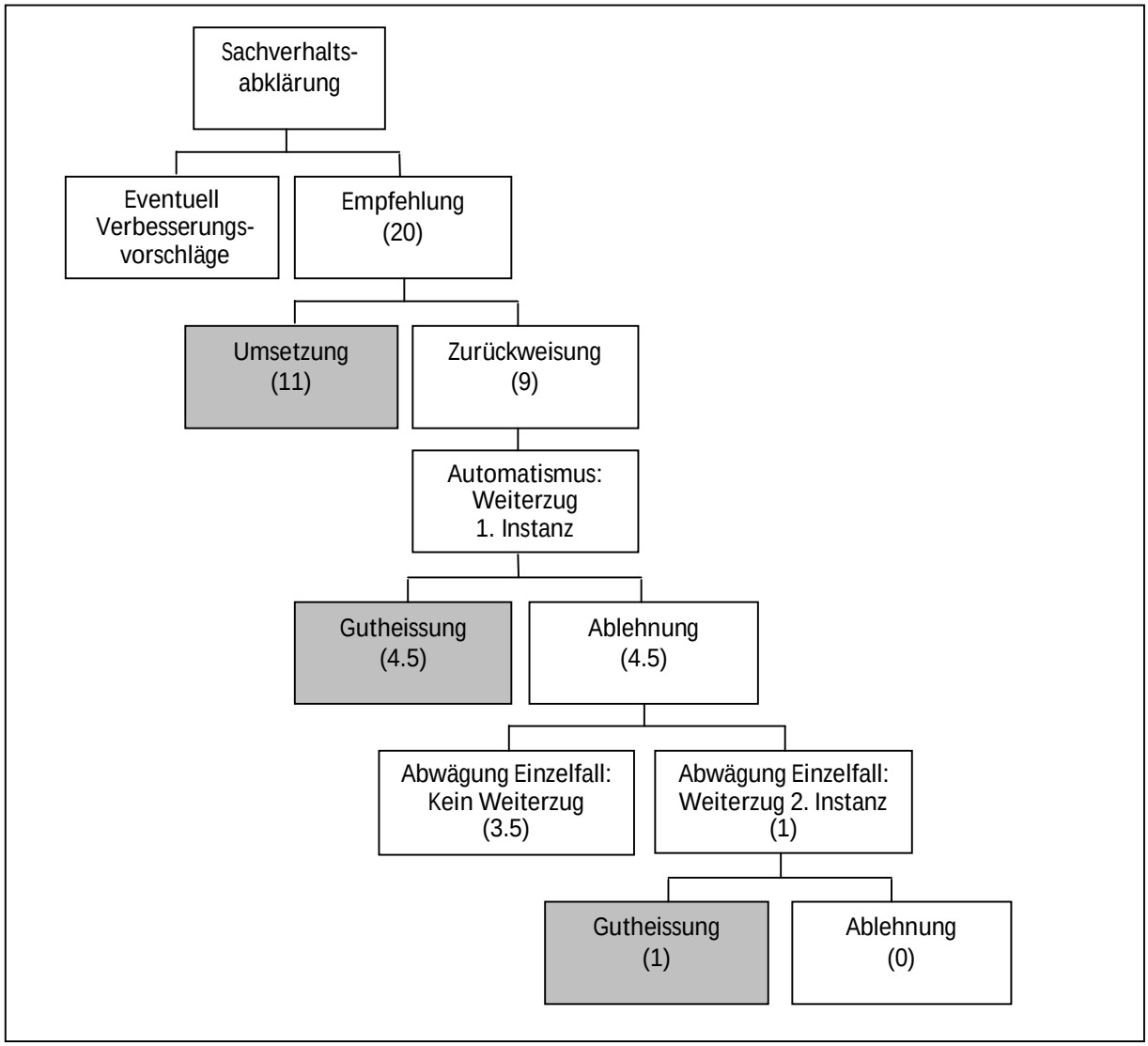
Die konsequente Anwendung dieser Strategie dürfte teilweise erklären, weshalb die Fallzahl insgesamt eher klein ist: Entscheidet sich der EDÖB, eine Empfehlung zu erlassen, so kann der Aufwand im Falle eines (nicht unwahrscheinlichen) Weiterzugs gross werden, wie sich in den Fällen *Google Street View* und *Logistep* gezeigt hat. Dies erfordert eine sorgfältige Abwägung, ob eine Empfehlung formuliert werden soll oder nicht. Neben der Bindung von Ressourcen ist bei Gerichtsverfahren auch zu berücksichtigen, dass deren zeitlicher Verlauf schwer planbar ist und vom EDÖB zusätzlich Flexibilität erfordert. Die Fallstudien haben gezeigt, dass die Beanspruchung im Falle eines Weiterzugs Ressourcen bindet, die an anderer Stelle fehlen.

Die Erfolgsaussichten im Falle eines Weiterzugs können als ambivalent beurteilt werden: Von den neun Fällen, in denen eine Entscheidung vorliegt, wurde die Position des EDÖB viermal vollständig und in einem Fall teilweise gestützt; in den verbleibenden vier Fällen wurde die Klage abgewiesen (Abbildung 12-7). Inwieweit dieses Vorgehen präventiv wirkt oder dazu beiträgt, dass Datenbearbeiter eine erlassene Empfehlung eher umsetzen, da sie andernfalls *immer* mit einem Weiterzug rechnen müssen, kann zahlenmässig nicht belegt werden. Zumindest theoretisch erscheint ein solcher Effekt jedoch plausibel, und auch die Interviewaussagen von Vertretern des EDÖB deuten in diese Richtung.

Während im Falle des Weiterzugs einer Empfehlung an die erste Instanz von einem Automatismus gesprochen werden kann, erweist sich die Situation nach dem rechtskräftigen Entscheid der ersten Instanz unterschiedlich: Nur im Fall *Logistep* hat der EDÖB bisher (erfolgreich) Beschwerde gegen den Entscheid geführt. Gemäss den Gesprächsaussagen war man beim EDÖB dabei von der Widerrechtlichkeit der Datenbearbeitung überzeugt; zudem war man der Meinung, dass vom Entscheid des BVGer über den Fall *Logistep* hinaus negative Signale ausgehen, inwiefern ein privates Interesse als Rechtfertigungsgrund für eine Datenbearbeitung angeführt werden kann. In den übrigen drei (resp. vier, wenn man den nur teilweise gut geheissenen Weiterzug mitzählt) Fällen wurde auf eine Beschwerde verzichtet. Dies lässt auf ein fallspezifisches Vorgehen in dieser Situation schliessen; beispielsweise verzichtete der EDÖB in einen Fall auf eine Beschwerde, weil das negative Urteil dennoch zur Klärung der Rechtslage beigetragen habe. Im Falle geringer Erfolgsaussichten vor Gericht und angesichts ressourcenintensiver Gerichtsverfahren scheint es sinnvoll, wenn Weiterzüge bis vor die letzte Instanz sorgfältig abgewogen werden.

Insgesamt kann der EDÖB in einer Mehrheit der Fälle eine Empfehlung direkt oder indirekt durchsetzen. Von den 20 Empfehlungen, deren Umsetzung im Rahmen dieser Evaluation abschliessend beurteilt werden kann, wurden 16 vollständig umgesetzt; in einem Fall wurde dem Anliegen des EDÖB teilweise nachgekommen (graue Flächen in Abbildung 12-7).

Abbildung 12-7: Vorgehen des EDÖB nach Sachverhaltsabklärungen



Eigene Darstellung. In Klammern sind die Anzahl Fälle angegeben, die sich den entsprechenden Kategorien zuordnen lassen. Drei von insgesamt 23 Empfehlungen wurden nicht berücksichtigt. Zwei Fälle sind noch vor der ersten Instanz hängig. Ein Fall wurde nach der Zurückweisung durch den Bearbeiter unter der Federführung der französischen Datenschutzbehörde weiterbearbeitet.

12.4.3 Wirkungen über den Einzelfall hinaus?

Wie weiter oben dargelegt wurde, achtet der EDÖB bei der Auswahl von Sachverhaltsabklärungen auch darauf, Fälle mit Mustercharakter zu berücksichtigen, deren Erkenntnisse somit auch auf andere Bearbeiter mit ähnlich gelagerter Problematik übertragen werden können. So konnte beispielsweise im Fall *Logistep* zur Klärung der Frage beigetragen werden, ob IP-Adressen als Personendaten betrachtet werden können. Auch konnte mit diesem Fall gemäss dem EDÖB gezeigt werden, dass die Tätigkeit von Privaten im Internet nicht schrankenlos erfolgen kann.

Ein wichtiger Hebel für den EDÖB, im Hinblick auf eine Wirkung über den Einzelfall hinaus ist die Veröffentlichung der Resultate einer Abklärung und der Empfehlungen im Tätigkeitsbericht,

im Internet oder auf anderen Kanälen, wie z.B. über eine Medienkonferenz. Allerdings verfügt der EDÖB gemäss Interviewaussagen kaum über die Mittel, um flächendeckend oder auch nur stichprobenweise zu kontrollieren, ob seine Vorgaben auch in anderen Unternehmen oder Bundesorganen tatsächlich umgesetzt werden. Entsprechende stichprobenweise Kontrollen seien zwar nicht auszuschliessen, kämen aber nur ausnahmsweise vor. Auch eine gezielte Information der jeweiligen Bearbeiter, die derselben Branche angehören (z.B. über Informationen an den Branchenverband) erfolgt nur in Ausnahmefällen.

Der EDÖB ist somit weitgehend darauf angewiesen, dass die angesprochenen Bearbeiter ihre allenfalls fehlbare Praxis von sich aus anpassen, oder aber von sensibilisierten Betroffenen oder den Medien dazu angehalten werden. Tatsächlich ist es laut den Interviewpartnern beim EDÖB schon vorgekommen, dass Bearbeiter nach einer Veröffentlichung um eine Beratung gebeten hätten oder dass er bei einem Verband oder im Rahmen eines Vortrags das Thema gezielt habe verbreiten können. Aus den Fallstudien ergeben sich gewisse Hinweise auf Wirkungen über den Einzelfall hinaus, die aber nur schwer verallgemeinerbar sind:

Im Fall *Mitarbeitercheck* konnte der EDÖB feststellen, dass nach der Gutheissung der provisorischen Massnahme vermehrt Firmen in Personalfragen auf den EDÖB zugekommen sind, was er als positiv wertet. Allerdings dürfte diese Wirkung nicht zuletzt mit Eigenschaften des Falls (erstmalige Anwendung der provisorischen Massnahme, rasches Einschreiten) zu tun haben und nur schwer zu verallgemeinern sein.

In der Fallstudie *Krankenversicherer* befragte der EDÖB alle obligatorischen Krankenversicherer zu deren datenschutzrechtlicher Situation. Damit unterscheidet sich das Vorgehen insofern von den anderen untersuchten Abklärungen und der Strategie, beispielhafte Fälle genau zu analysieren, als hier eine ganze Branche zur grundsätzlichen Umsetzung des Datenschutzes befragt wurde, um in einem zweiten Schritt datenschutzkritische Aspekte bei den Krankenversicherern genauer zu untersuchen. Ein auslösendes Moment für diese Studie waren datenschutzrechtliche Probleme bei einer einzelnen Kasse gewesen. Insofern kann die Umfrage als Versuch gelesen werden, einen Verdacht flächendeckend abzuklären. Allerdings geht man beim EDÖB nicht davon aus, dass in anderen Bereichen ähnlich vorgegangen werden kann. Im vorliegenden Fall ergab sich eine Situation, die das Vorgehen ermöglichte: Mit dem Bundesamt für Gesundheit (BAG) hatte eine andere Behörde ein Interesse an der und die Führungsrolle bei der Untersuchung, welche über die notwendigen Ressourcen und das erforderliche Know-how (fachlich, organisatorisch) verfügte. Allein sieht man sich der EDÖB nicht in der Lage, eine ähnliche Untersuchung durchzuführen.

Im Rahmen der Fallstudie *AVAM* kontrollierte der EDÖB das Bearbeitungsreglement eines Bundesorgans für eine Datensammlung. Neben der eigentlichen Überprüfung des Dokuments und der Formulierung von Verbesserungsmöglichkeiten zielt diese Aktivität auch darauf, dass sich die Inhaber von Datensammlungen vermehrt mit dem Datenschutz beschäftigen und sensibilisiert werden. Gemäss den Einschätzungen der Interviewpartner beim EDÖB gelingt ihm dies mit der Kontrolle von Bearbeitungsreglementen. Die Erfahrungen des interviewten Bearbeiters in diesem Fall vermögen diese Aussagen nur teilweise zu stützen. Demnach sei das Bearbeitungsreglement geeignet, um für die entsprechende Datensammlung Transparenz herzustellen und sich selber

Rechenschaft über die Datenbearbeitungen abzulegen. Dagegen wurde in diesem Gespräch keine Wirkung über das unmittelbar betroffene Projekt hinaus festgestellt.

Beim Fall *Google Street View* steht die Frage der Breitenwirkung nicht so sehr im Vordergrund, da Google der mit Abstand bedeutsamste Anbieter des entsprechenden Angebots ist.

Inwieweit von den Sachverhaltsabklärungen somit Wirkungen über den Einzelfall hinaus ausgehen, bleibt somit sowohl für den EDÖB selbst als auch für die Evaluation in vielen Fällen unklar. Es kann vermutet werden, dass die Breitenwirkung mit der Publizität des Falls zunimmt, da diese die Sensibilisierung der Betroffenen und der Bearbeiter fördern. Dass der EDÖB von sich aus, das heisst ohne konkrete Beschwerden von mehreren Betroffenen eine Stichprobenkontrolle bei einem Bearbeiter aus der gleichen Branche macht, muss dieser jedoch nicht befürchten. In der Regel wird er vom EDÖB auch nicht direkt oder über seinen allfälligen Branchenverband über die Ergebnisse einer Sachverhaltsabklärung orientiert.

12.5 Informationstätigkeit des EDÖB

Der vorliegende Abschnitt beschäftigt sich mit den Fragen, wann und wie der EDÖB die Öffentlichkeit informiert, wie die Qualität der Informationsprodukte bewertet wird sowie welche Wirkung die Informationstätigkeit möglicherweise entfaltet. Sein Informationsauftrag stützt sich auf Art. 30 DSG. Die Beantwortung der Fragen stützt sich auf die Homepage des EDÖB, auf Interviews mit den Datenbearbeitern, Experten und Interessenvertretern, den Interviews mit den Mitarbeitern des EDÖB sowie den drei Fallstudien, die zur Informationstätigkeit durchgeführt worden sind (*Leitfaden Überwachung, Mobile Computing* und *Soziale Netzwerke*).

12.5.1 Berichterstattung: Tätigkeitsberichte

Das DSG verpflichtet den EDÖB, regelmässig über seine Tätigkeit Bericht zu erstatten. Der EDÖB kommt dieser Verpflichtung mit den jährlich publizierten Tätigkeitsberichten nach. Über die Inhalte des Berichts entscheidet der EDÖB selbständig, so dass dieser nicht als Rechenschafts- oder Geschäftsbericht im engeren Sinn aufgefasst werden kann, sondern selektiv über Aktivitäten informiert, welche der EDÖB für öffentlichkeitsrelevant hält. Sämtliche im Rahmen des internationalen Rechtsvergleichs untersuchten Staaten können die Öffentlichkeit informieren (SIR 2010).

12.5.2 Öffentlichkeitsarbeit: Homepage des EDÖB

Der EDÖB kann die Öffentlichkeit unabhängig über diejenigen datenschutzrechlichen Anliegen informieren, die er als wichtig erachtet (vgl. Huber 2006: 404). Diese Aufgabe nimmt der EDÖB insbesondere mit der umfangreichen Homepage[251] wahr. Dort veröffentlicht er die meisten seiner Informationen und Stellungnahmen. Verschiedenen Interviewaussagen zufolge ist das Informationsangebot auf der Homepage in den vergangenen Jahren systematisch ausgebaut worden; ein

[251] http://www.edoeb.admin.ch bzw. http://www.derbeauftragte.ch.

zentraler Grund dafür ist die damit beabsichtigte Entlastung der Beratung (vgl. Ziffer 12.6.3). Folgende Publikationen können unterschieden werden:

- *Leitfäden* geben betroffenen Personen und Datenbearbeitern Hinweise, wie eine rechtsmässige Datenbearbeitung zu gestalten ist. Auf der Homepage sind momentan acht Leitfäden publiziert.
- *Merkblätter und FAQ-Beiträge* verfasst der EDÖB zu häufig gestellten Fragen. Die in Merkblättern hier angesprochenen Themen werden umfangreicher als häufige Fragen (FAQ) behandelt. Es gibt bislang acht Merkblätter; FAQ-Beiträge existieren zu zwölf unterschiedlichen Kategorien.
- Im *Newsletter* werden zweimal jährlich aktuelle Themen kurz dargestellt und konkrete Hinweise gegeben, wie man die Privatsphäre schützen kann.
- Für die Durchsetzung ihrer Rechte stehen den Betroffenen elf *Musterbriefe* zur Verfügung.
- *Empfehlungen und Weiterzüge* werden ebenfalls im Internet publiziert (vgl. oben).
- *Weitere Publikationen* sind Beiträge in der Fachpresse und Referate.

Im Folgenden soll kurz die Struktur der Homepage beschrieben werden. Von der Startseite aus lassen sich folgenden Kategorien erreichen:

- Unter *„Aktuell“* informiert der EDÖB über laufende Aktivitäten (Abschluss einer Abklärung, Veröffentlichung des Tätigkeitsberichts, Empfehlungen).
- In der Rubrik *„Themen“* finden sich verschiedene Informationen (z.B. Leitfäden, Empfehlungen, häufige Fragen, etc.) zu einzelnen Bereichen (z.B. Arbeitsbereich), aber auch konkrete Datenbearbeitungen (z.B. Videoüberwachung) oder Informationen zu einzelnen Artikeln des Datenschutzgesetzes (z.B. Datenschutzzertifizierung). Dabei finden sich Informationen zu klassischen wie auch zu neuen, unübersichtlicheren Konstellationen (z.B. *Soziale Netzwerke, Mobile Computing*).
- Die Rubrik *„Dokumentation“* ist nach den oben beschriebenen verschiedenen Informationsprodukten strukturiert. Weiter enthält sie Medieninformationen und Links zu anderen Akteuren im Bereich Datenschutz.
- Eher von praktischer Bedeutung sind die unter der Rubrik *„Dienstleistungen“* zur Verfügung gestellten Musterbriefe für Auskunftsbegehren beim Inhaber einer Datensammlung sowie Formulare zum Anmelden einer Datensammlung oder für die Anmeldung der Übermittlung von Personendaten ins Ausland. Schliesslich besteht an dieser Stelle die Möglichkeit, den EDÖB mittels eines Kontaktformulars direkt eine Frage zu stellen oder eine Meldung zu hinterlassen.

Insgesamt wurde http://www.edoeb.admin.ch inklusive Unterseiten im Jahr 2010 gemäss der Jahresstatistik von rund 163'000 Personen (resp. IP-Adressen) besucht; dies entspricht rund 2.5%

der Bevölkerung ab 15 Jahren[252]. Die Besucher frequentierten die Seite im Durchschnitt 1.5 Mal. Die Verweildauer eines Besuchs betrug im Durchschnitt knapp 5 Minuten, wobei 67.4% der Besuche maximal 30 Sekunden dauerten. Auch wenn aufgrund dieser Nutzungsziffern nicht auf einen sehr starken Sensibilisierungseffekt der Homepage geschlossen werden kann, so kann doch davon ausgegangen werden, dass die Informationen des EDÖB nachgefragt werden und ein professionell aufbereitetes und breites Informationsangebot gerechtfertigt scheint.

Die zeitliche Entwicklung der Nutzungsstatistik wurde im Rahmen der Evaluation nicht untersucht. Im Interview mit den Mitarbeitern des EDÖB gehen diese davon aus, dass deren Nutzung parallel zur allgemein steigenden Nutzung des Internet zugenommen hat. Sie stützen ihre Aussagen auf die Nutzungsstatistik, aber auch auf Aussagen von Personen, die die Seite im Rahmen der Beratung konsultieren und von Journalisten. Die Nutzer äusserten sich in der Regel zufrieden. Die Beiträge der EDÖB-Internetseite würden auch in Fachbeiträgen zitiert.

12.5.3 Nutzen der Informationen für Bearbeiter und Rechtsprechung

Der Internetauftritt und weitere vom EDÖB zur Verfügung gestellte Informationen werden von den befragten Datenbearbeitern als sehr nützlich eingestuft. Für etliche Interviewpartner ist die Homepage die erste Anlaufstelle bei Fragen zum Datenschutz. Im Besonderen werden die Leitfäden des EDÖB gelesen (Videoüberwachung, Überwachung am Arbeitsplatz) und im Alltag verwendet, aber auch andere Produkte werden als nützlich für die Alltagsarbeit beurteilt (Tätigkeitsberichte, Checklisten). Ebenfalls erwähnt worden ist von Seiten der privaten Datenbearbeiter, dass man sich in einigen Bereichen zusätzliche Leitfäden für Bearbeitungen wünscht, was ebenfalls auf eine hohe Nützlichkeit der bereits bestehenden Informationen hinweist, gleichzeitig aber auch andeutet, dass der EDÖB auf seiner Internetseite nicht alle Informationsbedürfnisse befriedigen kann. Ähnlich wie bei den Beratungen werden auch die Publikationen des EDÖB, obwohl ihnen keine Verbindlichkeit im rechtlichen Sinne zukommt, in der Praxis als verbindliche Leitlinien betrachtet. Es sei an dieser Stelle einschränkend noch einmal erwähnt, dass die befragten privaten Datenbearbeiter wohl als überdurchschnittlich sensibilisiert bezeichnet werden können, so dass sich diese Befunde nicht verallgemeinern lassen.

Neben der insgesamt sehr positiven Gesamtbeurteilung wurden kritische Kommentare bezüglich der Übersichtlichkeit und Darstellung der Homepage abgegeben. Beim EDÖB erklärt man diesbezüglich, dass man den Webauftritt nicht völlig frei gestalten könne, sondern sich an die Vorlage des Bundes zu halten habe. Zu prüfen wäre allenfalls die Möglichkeit eines eigenständigen Internetauftritts, der auch der Unabhängigkeit des EDÖB gegenüber den Bundesbehörden Ausdruck verleihen würde. Demgegenüber bringt die aktuelle Lösung zum Ausdruck, dass es sich um eine Bundesbehörde handelt, was möglicherweise vertrauensbildend sein kann.

Nach Auskunft der Interviewpartner beim EDÖB werden die von ihm veröffentlichten Stellungnahmen in der Fachdiskussion und im Rahmen der Rechtsanwendung durch die Gerichte als Interpretationshilfen benützt und haben einen entsprechend hohen Stellenwert, der mit jenem der rechtswissenschaftlichen Fachliteratur ähnlich sei. Der Unterschied sei, dass die Interpretati-

[252] Ständige Wohnbevölkerung der Schweiz 2009 gemäss Bundesamt für Statistik (ESPOP): 6'604'600 Personen.

on der Behörde einen etwas offizielleren Charakter habe. Bei Divergenzen bestehe vielleicht eine kleine Tendenz, die EDÖB-Stellungnahmen höher zu gewichten als einen Beitrag von jemandem, der weniger bekannt ist.

12.5.4 Öffentlichkeitsarbeit: Medienkontakte und weitere Aktivitäten

Besondere Bedeutung in der Informationstätigkeit des EDÖB kommt den Medien zu. Anlässlich der Publikation seines jährlichen Tätigkeitsberichts veranstaltet er eine Medienkonferenz und versucht dort, die wichtigsten aktuellen Themen den Medien anzubieten. Darüber hinaus informiert er aus aktuellem Anlass sporadisch aktiv mit eigenen Medienmitteilungen; dies geschieht meistens im Rahmen seiner Aufsichtstätigkeit (Empfehlungen, Weiterzüge, Urteile) oder aber es handelt sich um Hinweise in eigener Sache (Publikation Tätigkeitsbericht, Tagungen). 2009 etwa publizierte er sieben Medienmitteilungen, 2008 deren fünf und 2007 deren drei. 2009 fand zum Thema Google Street View überdies eine extra einberufene Medienkonferenz statt.

Den vermutlich höheren Anteil der Medienpräsenz machen allerdings Auskünfte, Interviews und Stellungnahmen des EDÖB im Rahmen von themenspezifischen Medienanfragen aus. Der Eindruck beim EDÖB und auch der übrigen Interviewpartner ist es, dass die Medienpräsenz des EDÖB in den vergangenen Jahren zugenommen hat. Die Medienpräsenz ist stark auf den Leiter der Behörde, Hanspeter Thür, fokussiert, der schon vor Amtsantritt als Nationalrat eine bekannte Persönlichkeit war. Gegen aussen tritt der „Beauftragte“ so mit einem bekannten Gesicht auf, was es ihm erleichtern dürfte, im stark personalisierenden Mediensystem Beachtung zu finden. Es wurde nicht systematisch überprüft, ob ihm dies in allen Sprachräumen gleich gut gelingt. Der Befund der Bevölkerungsumfrage, wonach der EDÖB in der Deutschschweiz deutlich bekannter ist als in der französischen und der italienischen Schweiz, könnte ein Hinweis darauf sein, dass dieser Anspruch nicht erfüllt wird.

Der EDÖB wünscht sich laut den Aussagen im Interview mehr Medienpräsenz. Es gelinge nicht bei allen Themen gleich gut, das Interesse der Journalisten zu wecken. Für die Darstellung der teils komplexen Zusammenhänge aus dem Datenschutzbereich sei oft zu wenig Platz, was zu Verkürzungen und Verzerrungen führe. Im Staatsschutzbereich, der breit diskutiert werde, sei die Offenheit grösser als anderswo. Die Medien sind für den EDÖB in doppelter Hinsicht relevant: Zum einen können sie durch ihre Berichterstattung Inputs für Aktivitäten des EDÖB liefern, zum anderen transportieren sie Informationen in die Bevölkerung, und tragen so zur Sensibilisierung resp. zur Wirksamkeit der Aufsichtstätigkeit bei.

Zu den weiteren Informationstätigkeiten des EDÖB können zum einen Auftritte des EDÖB oder seiner Mitarbeiter vor einem jeweils beschränkten Publikum im Rahmen von Konferenzen oder Unterlagen für Ausbildungen gezählt werden. Solche hat der EDÖB wie erwähnt durch die Universität Freiburg erstellen lassen. Daneben publizieren Mitarbeitende des EDÖB Fachartikel in einschlägigen Publikationen.

12.5.5 Auslösung und Durchführung von Informationsaktivitäten

Ähnlich wie im Fall von Sachverhaltsabklärungen kommt der Impuls im Falle von Informationen in der Regel von aussen (vgl. Tabelle 11-2): Bezüglich der durchgeführten Fallstudien waren es bei den *Sozialen Netzwerken* Betroffene oder Angehörige, bei *Mobile Computing* kleinere Unternehmen und beim *Leitfaden Überwachung* zunächst Arbeitnehmer, dann mehr und mehr auch Arbeitgeber, welche die Aktivität des EDÖB auslösten. Auch die Kriterien, die zu einer Aktivität führen, sind ähnlich wie im Falle einer Sachverhaltsabklärung: Potenziell viele Betroffene, sensible Daten sowie eine mediale, politische oder internationale Relevanz des Themas.

Im Fall *Soziale Netzwerke* war der EDÖB in der Situation, dass der Druck gross war, etwas zu unternehmen: Viele Personen sind betroffen, es handelt sich um sensible Daten, das Interesse der Medien und der Politik ist hoch. Die Information bezweckt, mögliche Probleme im Zusammenhang mit Sozialen Netzwerken aufzuzeigen und Empfehlungen für die Nutzer, die Anbieter und die Behörden bereitzustellen. Die Wahl zu Gunsten einer Information erklärt sich gemäss dem EDÖB dadurch, dass eine Sachverhaltsabklärung wenig erfolgversprechend wäre[253]: Seitens des EDÖB wird argumentiert, dass die Wirkung des schweizerischen DSG im Falle dieses globalen Problems begrenzt ist. In diesem Fall erweist sich die Information als „Auffangbecken", weil im Bereich der Aufsicht geringe Aussichten auf eine erfolgreiche Problembehandlung bestehen (vgl. Ziffer 12.6.2). Gleichzeitig ist festzuhalten, dass im Bereich der Sozialen Netzwerke das Potenzial des Selbstschutzes durch die Betroffenen viel höher ist als etwa im Fall *Google Street View*, weil die Betroffenen durch richtiges und vorsichtiges Verhalten wesentlich mitsteuern können, welche Daten von ihnen für Dritte zugänglich werden.

Die Fallstudien zur Information machen ebenfalls deutlich, dass der EDÖB darum bemüht ist, seine Informationen in Projekte anderer Akteure einzubringen. So konnte er unter anderem die erarbeiteten Informationen zu den Sozialen Netzwerken bei Kampagnen anderer Bundesämter (BAKOM und BSV) zum Thema Jugendliche und Internet einbringen. Eine solche Strategie ist angesichts der Ressourcenknappheit und auch aus fachlicher Sicht (Kombination von Know-how) zu begrüssen. Angesichts der Erkenntnisse der Fallstudien geschieht dies allerdings nicht systematisch und hauptsächlich auf Initiative des EDÖB.

12.6 Zusammenhänge zwischen den verschiedenen Aktivitäten

Bisher wurden die gesetzlichen Aufgaben der Beratung, Aufsicht und Information grösstenteils isoliert betrachtet. Vor allem in den Fallstudien hat sich jedoch gezeigt, dass zwischen den einzelnen Aufgaben Wechselwirkungen bestehen, welche nun in diesem Abschnitt thematisiert werden. Im weiteren ist die Doppelrolle des EDÖB gegenüber den Datenbearbeitern anzusprechen, muss er letztere doch einerseits beraten und damit unterstützen und andererseits beaufsichtigen und damit kontrollieren. Die Ausführungen stützen sich auf die Interviews mit Kaderleuten und Mitarbeitern des EDÖB sowie mit Datenbearbeitern sowie auf die Fallstudien.

---

253 Anders als im Fall *Google Street View* bearbeitet beispielweise Facebook (als international bedeutendstes Soziales Netzwerk) die Daten nicht in der Schweiz. Ebenfalls hat das Unternehmen keine Tochtergesellschaft in der Schweiz.

Tabelle 12-3 gibt einen Überblick darüber, welche Wechselwirkungen zwischen den Aktivitäten bestehen können. Dabei lassen sich zwei Situationen unterscheiden: Einerseits kann eine Aktivität eine andere auslösen (*Auslösung*); andererseits ist es auch möglich, dass eine Aktivität an Stelle einer anderen durchgeführt wird (*Substitution*). Weiter werden in der Tabelle Beispiele aus den Fallstudien aufgeführt, in denen der beschriebene Zusammenhang festgestellt werden kann. Sie werden in den folgenden Abschnitten näher erörtert.

Tabelle 12-3: Zusammenhänge zwischen verschiedenen Aktivitäten: Übersicht

	Aufsicht–Beratung	*Aufsicht–Information*	*Beratung–Information*
Auslösung	Beratungstätigkeit löst Sachverhaltsabklärung aus. Bsp. *SAKE*.	Sachverhaltsabklärung löst begleitende Informationstätigkeit aus. Bsp. Google, *Logistep*.	(Häufige) Beratungen lösen Informationstätigkeit aus. Bsp. *Mobile Computing*, *Leitfaden Überwachung*.
	Aufsichtstätigkeit löst Beratung aus. Bsp. *AVAM*, Krankenversicherungen.	Sachverhaltsabklärung löst Informationstätigkeit aus. Bsp. Leitfaden Überwachung.	
Substitution	-	Informationstätigkeit ersetzt Aufsicht. Bsp. *Soziale Netzwerke*.	Informationstätigkeit ersetzt Beratung. Bsp. *Mobile Computing*, *Leitfaden Überwachung*.

12.6.1 Aufsicht und Beratung

Anhand der Fallstudien lässt sich zeigen, dass sich aufgrund einer Beratung Aufsichtsaktivitäten ergeben können: Die Beratungstätigkeit des EDÖB im Fall *SAKE* hat zwei Sachverhaltsabklärungen ausgelöst: In einer ersten untersucht der EDÖB generell die Informationsschreiben des Amtes für Befragungen; die zweite Kontrolle bezieht sich auf die Rolle und Pflichten des BFS im Rahmen der Zusammenarbeit mit dem Umfrageinstitut. Im zweiten Fallbeispiel zur Beratung stand eine Sachverhaltsabklärung nicht zur Diskussion. Der Interviewpartner beim EDÖB bemerkte jedoch, dass man sich Fälle vormerke, in denen sensible Daten bearbeitet werden, um nach einer gewissen Zeit eine Nachkontrolle durchzuführen.

Der EDÖB verteidigt seine Doppelrolle. Das zentrale Gebot im Umgang damit sei die Fairness und Transparenz gegenüber den Beratenen, erläutern die befragten Mitarbeiterinnen und Mitarbeiter. Gemäss der Einschätzung des involvierten Amtes ist der EDÖB diesem Anspruch im Fall *SAKE* diesem Anspruch gerecht geworden. Der EDÖB kommuniziere im Rahmen der Beratung offen, dass er auch Aufsichtsorgan sei; er signalisiere den Befragten jeweils deutlich, dass er sich vorbehalte, später auch zu überprüfen, ob der Bearbeiter seine Anwendung tatsächlich auch rechtskonform gemäss seinen Ratschlägen umgesetzt habe, und gegebenenfalls zu intervenieren. Dies lässt die teilweise wahrgenommene Zurückhaltung der Privaten, den EDÖB für Beratungen zu konsultieren, als plausibel erscheinen. Gleichzeitig gelte es bei der Frage nach dem Verhältnis zwischen Aufsicht und Beratung aber zu berücksichtigen, dass eine wichtige Voraussetzung für

eine erfolgreiche Beratung das gegenseitige Vertrauen sei. In diesem Sinne wäre es nicht förderlich, von Anfang an mit einer Sachverhaltsabklärung zu drohen.

Umgekehrt kann sich aus der Kontrolltätigkeit auch die Beratung von Akteuren ergeben. So wird im Fallbeispiel zur Krankenversicherung nach der Erhebung der datenschutzrechtlichen Situation bei den Versicherern vom EDÖB betont, dass er den Versicherungen bei Verbesserungsmassnahmen im direkten Anschluss an die Erhebung beratend zur Seite stehe. Auch bei der Kontrolle eines Bearbeitungsreglements (Fall *AVAM*) sieht sich der EDÖB Interviewaussagen zufolge, sofern keine gravierenden Mängel vorhanden sind oder noch gar kein Reglement besteht, eher in der Rolle des Beraters und weniger als Kontrollorgan.

Insgesamt ergibt sich aus diesen Ausführungen, dass die Beratungs- und die Aufsichtstätigkeit nicht zwei absolut voneinander getrennte Aktivitäten sind, sondern sich gelegentlich im gleichen Fall ergänzen und ablösen. Es ist davon auszugehen, dass der EDÖB seine Doppelrolle als beratende und beaufsichtigende Behörde für die Bearbeiter transparent und damit fair ausübt. Der Preis der Doppelrolle ist, dass Bearbeiter eine Beratung durch den EDÖB bisweilen vermeiden, um ihn nicht auf mögliche datenschutzrechtliche Probleme aufmerksam zu machen.

12.6.2 Aufsicht und Information

Die Informationstätigkeiten des EDÖB sind im Rahmen von Sachverhaltsabklärungen als wichtiges Unterstützungsmittel zu betrachten. Der EDÖB macht jene Fälle, in denen es zu Empfehlungen oder Gerichtsverfahren kommt, öffentlich, was vor allem im Privatbereich das Image eines Unternehmens schädigen kann. Die Information soll in diesen Fällen die Wirksamkeit der Aufsichtstätigkeit verstärken; der EDÖB erhofft sich damit auch eine gewisse präventive Wirkung auf andere Datenbearbeiter.

Die Fallstudien zu Sachverhaltsabklärungen aus dem Privatbereich, bei denen es zu einem Gerichtsverfahren gekommen ist (*Logistep, Google Street View*), veranschaulichen dies. Gleichzeitig betonen die Interviewpartner beim EDÖB, dass der EDÖB in denjenigen Fällen, in denen sich die Datenbearbeiter kooperativ verhalten und seine Verbesserungsvorschläge umsetzen, die Öffentlichkeit sehr zurückhaltend informiere resp. sogar dazu bereit sei, ein Unternehmen für die getätigten Anstrengungen positiv zu würdigen. Zu beachten gilt es in diesem Fall, dass durch eine zurückhaltende Information eine allfällige Auswirkung auf andere Bearbeiter schwieriger zu erzielen ist.

Dennoch erscheint das Vorgehen vor dem Hintergrund des Imagerisikos, das für einen Datenbearbeiter bei negativer Publizität besteht, als sinnvoll: Es bietet für die betroffenen Unternehmen und Bundesorgane einen Anreiz zur Kooperation; gleichzeitig kann damit der ressourcenintensive Gerichtsweg unter Umständen vermieden werden. Die Interviewpartner beim EDÖB vermuten, dass in bestimmten Fällen das Imagerisiko für den Datenbearbeiter den grösseren Anreiz für ein DSG-konformes Verhalten darstelle als eine mögliche Sanktion.

Eine zweite Möglichkeit, wie die Aufsichtstätigkeit eine Informationstätigkeit auslösen kann, zeigt sich anhand der Fallstudie *Leitfaden Überwachung*. Die Erfahrungen im Rahmen von Sachver-

haltsabklärungen lieferten Hinweise auf virulente Probleme in diesem Bereich und bewirkten nebst anderen Faktoren die Publikation eines generalisierten Leitfadens zum Thema.

Daneben bildet die Information ein Auffangbecken in Bereichen, in denen die Aufsichtsfunktion wie im Fall der *Sozialen Netzwerke* ins Leere läuft: Hierbei geht es vor allem um praktische Tipps für Betroffene, wie sie sich am wirksamsten gegen die Gefahren von Sozialen Netzwerken schützen können. Zur Wirksamkeit dieses Vorgehens lassen sich keine empirisch fundierten Ergebnisse festhalten.

12.6.3 Beratung und Information

Zwischen der Beratungstätigkeit und der Information besteht ein enger Zusammenhang. Auf der einen Seite können verschiedene Anfragen und Beratungen in einem Bereich dazu führen, dass der Entschluss gefasst wird, Erläuterungen, Leitfaden oder ein anderes Produkt zu verfassen. Im Fall *Mobile Computing* etwa führten verschiedene Anfragen von Kleinunternehmen, denen das technische Know-How in diesem Bereich fehlte, zur Ausarbeitung eines Informationspapiers beim EDÖB. Dem *Leitfaden Überwachung* am Arbeitsplatz gingen unter anderem Anfragen von verschiedenen Arbeitgebern voraus, die vom EDÖB wissen wollten, wie sie in diesem Bereich vorzugehen hatten.

Auf der anderen Seite unterstützen Informationsprodukte die Beratungstätigkeit, indem sie innerhalb der Organisation des EDÖB erarbeitetes Wissen festhalten und damit die Durchführung von Beratungen effizienter gestalten. Die Erläuterungen zu *Mobile Computing* etwa dienen nicht zuletzt auch den Mitarbeitern des EDÖB, die sich im Rahmen ihrer Beratungstätigkeit mit solchen Fragen auseinandersetzen müssen. Zudem besteht die Möglichkeit, dass sich interessierte Betroffene und Bearbeiter selber informieren können, und damit auch den EDÖB entlasten. So kann der EDÖB bei der Beratung oftmals zunächst auf bereits publizierte Informationen verweisen (FAQ, Merkblätter, Leitfäden, weitere). Im Interview betonte der Chef EDÖB, dass mit dem Entschluss, die Beratungstätigkeit zu kanalisieren, eine Stärkung der Informationstätigkeiten einhergegangen sei.

12.7 Stellungnahmen des EDÖB im Rahmen der Rechtsetzung

Dieser Abschnitt widmet sich den Stellungnahmen des EDÖB im Rahmen der Rechtsetzung. Dazu werden Interviewaussagen sowie die Auswertung der Tätigkeitsberichte herangezogen. Eine vollständige Übersicht über alle dem EDÖB zugeleiteten Gesetzgebungsvorlagen und seine Stellungnahmen existiert nicht.

Gemäss Art. 31 Abs. 1 Bst. b DSG nimmt der EDÖB Stellung zu Vorlagen über Erlasse und Massnahmen des Bundes, die für den Datenschutz erheblich sind. Nach den Aussagen der Interviewpartner beim EDÖB erhält dieser tatsächlich mit wenigen Ausnahmen alle datenschutzrelevanten Vorlagen im Rahmen der Ämterkonsultation zur Kenntnis. Einige Departemente schickten einfach alle Erlasse auch dem EDÖB, was zu einer aufwendigen Triage führe; andere Departemente schicken nur die wirklich relevanten Dossiers. Darüber hinaus achte auch die Bundeskanzlei auf die Frage, ob eine Vorlage datenschutzrelevant sei und beliefere den EDÖB. Nur

ausnahmsweise erfahre man auf anderen als diesen offiziellen Kanälen von einem gesetzgeberischen Vorhaben.

Wie die Interviewpartner versicherten, werden beim EDÖB alle eingehenden Projekte begutachtet. Wenn der EDÖB sich ausserstande sehe, fristgerecht zu antworten, ersuche er um Fristerstreckung. Wenn diese nicht gewährt werde, behalte er sich vor, zu einem späteren Zeitpunkt des Entscheidungsprozesses einzugreifen. Es komme auch vor, dass man sich im parlamentarischen Verfahren an die vorberatenden Kommissionen wende. Bisweilen wird der EDÖB auch von der parlamentarischen Kommission konsultiert. Wie es im Verfahren der Ämterkonsultation üblich ist, nehme man nur Stellung, wenn man etwas zu beanstanden habe.

Pro Jahr dürften deutlich mehr als hundert solcher Vorlagen beim EDÖB zur Stellungnahme eingehen. Die Interviewpartner schätzen, dass der EDÖB etwa bei der Hälfte der Projekte substanzielle Einwände mache. Sie beobachten heute seltener als in früheren Jahren, dass in einer an sich datenschutzrelevanten Vorlage der Datenschutz gar nicht thematisiert werde. Dies zeige, dass das Bewusstsein für den Datenschutz zugenommen habe. Die Befragten gaben auch eine grobe Schätzung darüber ab, was die Einwände des EDÖB bewirken. Häufig würden diese teilweise, aber nicht vollständig berücksichtigt. Rund ein Fünftel der Beanstandungen würden überhaupt nicht berücksichtigt. Als zentrales Anliegen bezeichneten es die Befragten beim EDÖB, dass dessen Haltung im Vernehmlassungsbericht explizit gemacht werde.

13 Zusammenfassung und Fazit zum EDÖB

Dieses Kapitel zieht Bilanz zu den Befunden über die organisatorischen Aspekte und die Wirksamkeit des EDÖB. In einem ersten Abschnitt wird versucht, basierend auf den Erkenntnissen der vorangehenden Kapitel die Gesamtstrategie des EDÖB nachzuzeichnen. Im zweiten Teil werden weitere Befunde zusammengefasst, welche sich auf die Organisation des EDÖB beziehen. Im dritten Teil wird die Wirksamkeit des EDÖB in den wichtigsten Aktivitätsfeldern und vor dem Hintergrund der technologischen Entwicklung diskutiert.

13.1 Strategie des EDÖB

Das DSG und die VDSG enthalten neben der Aufzählung der verschiedenen Aufgaben des EDÖB keine konkretisierenden Bestimmungen über die Gewichtung der verschiedenen Aufgaben oder gar Zielvorgaben für den EDÖB. Als unabhängige Behörde geniesst er hinsichtlich der Wahl seiner Strategie somit eine grosse Freiheit. Ein eigentliches Strategiedokument oder ein Leitbild hat sich der EDÖB nicht gegeben, zumindest existiert kein öffentlich zugängliches entsprechendes Dokument. Die nachfolgend aufgeführten Merkmale seiner Arbeitsweise ergeben sich aus den vorstehenden Kapiteln und damit aus den hierzu verwendeten Quellen.

- *Input-orientiertes Verhalten:* Der EDÖB gibt an, dass er sich bei der Auswahl der Fälle über weite Strecken input-orientiert verhalten müsse: Dabei orientiert er sich nach seiner Darstellung an Hinweisen und Klagen aus der Bevölkerung und an Themen, die sich aus der Beratung der Bearbeiter und der Befragten ergeben. Er stützt sich nicht allein auf Einzelfälle, sondern beobachtet auch die Entwicklung anhand der Themen, die in der Fachwelt diskutiert werden, anhand der politischen Geschehnisse und anhand der öffentlichen Diskussion in den Medien, um auf konkrete Anfragen vorbereitet zu sein. Auch verarbeitet er Hinweise anderer Behörden. Das gegenwärtige stark inputorientierte Vorgehen entspricht der vorgegebenen Marschroute des DSG, das insbesondere im Bereich der privaten Aufsicht Abklärungen nur bei einem bestehenden Verdachtsmoment vorsieht.

- *Rollende Planung der Schwerpunkte:* Basierend auf seinen Beobachtungen versucht der EDÖB nach seiner Darstellung, im Rahmen einer Mehrjahresplanung die relevanten kommenden Themen früh zu erkennen, um rechtzeitig auf die damit verbundenen Probleme vorbereitet zu sein. Jährlich werden im Voraus Schwerpunkte festgesetzt und nachher im Rahmen einer rollenden Planung kontrolliert, inwieweit die tatsächliche Arbeit diesen gerecht wird.

- *Kriterienbezogene Priorisierung:* Die Triage und Priorisierung der vom EDÖB behandelten Themen und Einzelfälle orientiert sich einerseits an diesen Schwerpunkten, andererseits nach klaren Relevanzkriterien, die sich aus dem Gesetz ableiten lassen. Entscheidend sind insbesondere die Anzahl der von der Aktivität eines oder mehrerer vergleichbarer Bearbeiter betroffenen Personen, die Schwere der damit einhergehenden Persönlichkeitsverletzung oder eine Kombination der beiden Kriterien. Auch politische Überlegungen geben bisweilen den

Ausschlag für oder wider eine vertiefte Fallabklärung. Gemäss der Literatur legt der EDÖB seinen gesetzlichen Spielraum insbesondere bei der Beaufsichtigung von Privaten weit aus; inhaltlich sind die Kriterien, die er für die Durchführung einer Sachverhaltsabklärung heranzieht, jedoch nachvollziehbar.

- *Exemplarische Fälle:* Das gegen Aussen sichtbare Handeln des EDÖB ist somit stark von einer Einzelfalloptik geprägt. Der EDÖB bearbeitet insbesondere im Bereich der Aufsicht (aber auch der Information) gezielt Fälle und Themen, die eine gewisse Brisanz aufweisen und in der öffentlichen Diskussion stehen, was ihm und damit der Thematik des Datenschutzes eine erhöhte Aufmerksamkeit verleiht. Dabei versucht er insbesondere, datenschutzrechtliche Grundsatzfragen zu beantworten. Aufgrund der Ressourcensituation (vgl. Ziffer 11.3) ist es dem EDÖB nicht möglich, potenzielle Missstände flächendeckend zu bearbeiten, sondern er muss sich auf beispielhafte Fälle konzentrieren. Bei denjenigen Fällen, die er untersuchen kann, führt er jedoch gründliche Abklärungen durch und schöpft die ihm zur Verfügung stehenden Rechtsmittel (Empfehlungen, Rechtsweg) aus. Bei Fällen, bei denen EDÖB den Rechtsweg einschlägt, geht es oft nicht einzig darum, die Interessen des Datenschutzes durchzusetzen, sondern auch eine rechtlich abschliessende Klärung durch ein Gericht herbeizuführen.

- *Öffentlichkeit als Hebel:* Die Publikation von Missständen durch den EDÖB erfüllt einen doppelten Zweck. Erstens ist sie aus Imagegründen ein wichtiger Motivator der involvierten Datenbearbeiter, sich zu verbessern. Zweitens soll sie die Betroffenen für das jeweilige datenschutzrechtliche Problem sensibilisieren, um den Druck für Verbesserungen bei vergleichbaren Datenbearbeitern zu verstärken.

- *Konstruktiv-kritische Grundhaltung:* Der EDÖB vertritt die Haltung, er habe in der Öffentlichkeit nicht das Image eines Verhinderers oder eines Verfechters fundamentalistischer Positionen. Diese Auffassung wird mit nur wenigen Abstrichen auch von den anderen Interviewpartnern weitgehend geteilt und ergibt sich auch aus dem Studium der EDÖB- Dokumente und seiner Arbeitsweise: Bevor der EDÖB auf den Verzicht einer bestimmten Datenbearbeitung drängt, sucht er in aller Regel nach Vorschlägen für eine DSG-konforme Bearbeitung. Gleichzeitig appelliert er nicht allein ans Gesetz, sondern an die Interessen und Anreize der Bearbeiter für eine datenschutzkonforme Bearbeitung.

- *Gewichtung und Verzahnung der Hauptaktivitäten:* Aufgrund der vorliegenden Daten kann davon ausgegangen werden, dass der EDÖB auf ein ungefähr ausgewogenes Verhältnis seiner Aktivitäten mit Bezug auf die privaten und die öffentlichen Datenbearbeiter achtet. Ebenfalls scheint die Wahl der Sachbereiche, soweit sie steuerbar ist, gut begründet. Auf alle drei Hauptaktivitäten (Aufsicht, Beratung, Information) verwendet der EDÖB einen namhaften Anteil seiner Ressourcen. Er hat in den vergangenen Jahren Bemühungen unternommen, die Beratung zu rationalisieren, um der Aufsicht mehr Zeit widmen zu können; der vorgesehene Abbau der Beratung von Bundesbehörden liess sich jedoch nicht vollständig umsetzen. Der Anteil der Aufsicht ist nach Ansicht des EDÖB eher noch auszubauen. In der täglichen Arbeit sind die drei Hauptaktivitäten eng verzahnt, wie die Evaluation gezeigt

hat. Die Preisgabe eines der drei Pfeiler würde somit auch die Wirksamkeit der anderen Pfeiler beeinträchtigen.

Insgesamt ergibt sich aus den Ausführungen das Bild einer im Rahmen ihrer beschränkten Ressourcen zielorientiert und wirksam handelnden Aufsichtsbehörde. Die Organisationsstruktur und die Abläufe sind effizient und zielführend, erlauben sie doch einen geordneten Informationsfluss und im Sinne des DSG wohlbegründete Planungs- und Priorisierungs-Entscheide. Wie konsequent die aus den Dokumenten und im Rahmen von Interviews erhobene Strategie des EDÖB in der alltäglichen Praxis tatsächlich umgesetzt wird, konnte in dieser Evaluation nicht untersucht werden.

13.2 Weitere Befunde zur organisatorischen Aspekten der Aufsichtsbehörde

Weitere wichtige Befunde zu organisatorischen Aspekten der Aufsichtsbehörde können wie folgt zusammengefasst werden:

- *Unabhängigkeit:* Die Weisungsunabhängigkeit ist ein zentraler Pfeiler der Wirksamkeit des EDÖB, insbesondere da, wo er Aufsichtstätigkeiten ausübt. Im Rahmen der jüngsten Gesetzesrevision, die am 1. Dezember 2010 in Kraft getreten ist, ist die Unabhängigkeit formell etwas gestärkt worden, da der Bundesrat nicht mehr das abschliessende Wahlrecht geniesst, sondern das Parlament seinen Wahlvorschlag genehmigen muss. Weitere neue Vorschriften haben zu einer Klärung des Arbeitsverhältnisses und der Bedingungen seiner Auflösung geführt. Im internationalen Vergleich entspricht die aktuelle Stellung des EDÖB weitgehend einem Normalfall, wobei in den meisten berücksichtigten Ländern nicht die Regierung als oberste Verwaltungsbehörde, sondern das Parlament oder das Staatsoberhaupt die Aufsichtsbehörde wählt. Aus dem Rechtsvergleich kann ergänzt werden, dass in mehreren Ländern die Datenschutzbehörde nicht hierarchisch organisiert ist, sondern durch ein Kollegialorgan geführt wird, was die Berücksichtigung verschiedener Interessengruppen und spezifischer Expertise erlaubt. In der Praxis sind schon unter der alten Rechtsordnung keine Fälle festgestellt worden, welche auf eine beeinträchtigte Unabhängigkeit des EDÖB schliessen liessen. Eine fortbestehende Lücke der Unabhängigkeit ist die Tatsache, dass der EDÖB seinen Budgetantrag lediglich durch die Bundeskanzlei vor dem Bundesrat verteidigen lassen, und seine Position auch im Parlament nicht selbst vorbringen kann (Beachte aber Art. 31. Abs. 1 VDSG). Eine solche Regelung ist jedoch im internationalen Vergleich nicht aussergewöhnlich.

- *Dokumentation der Aktivitäten:* Wie oben im Rahmen der Erläuterungen zur Strategie des EDÖB beschrieben, legt der EDÖB seinen Ressourceneinsatz planvoll, gezielt und anhand kriteriengesteuerter Prioritäten fest. Zu bemängeln ist hingegen die Transparenz seiner Schwerpunktfestlegung, des tatsächlichen Mitteleinsatzes und des Erfolgs. Anhand der verfügbaren Dokumente ist eine systematische Bilanzierung seiner Wirkungen nur begrenzt möglich. Auch in seiner Berichterstattung zuhanden der Öffentlichkeit bemüht sich der EDÖB kaum, die grossen Linien seiner Aktivitäten und der Erfolgsbilanz aufzuzeigen. Dies kann die Öffentlichkeit aber auch von einer weisungsunabhängigen Behörde verlangen;

gleichzeitig vergibt der EDÖB damit auch eine Chance, auf seine strukturellen Probleme und seine Erfolge hinzuweisen.

- *Zusammenarbeit mit anderen behördlichen Akteuren des Datenschutzes:* Angesichts der zunehmend grenzüberschreitenden Datenbekanntgaben und Dienstleistungsangebote im Internet wird die internationale Zusammenarbeit von Datenschutzbehörden immer wichtiger. Der EDÖB ist in den wesentlichen Organisationen in Europa und auf der weiteren internationalen Ebene gut eingebunden; insgesamt hinkt jedoch die internationale Kooperation der Datenschutzbehörden der Entwicklung und Internationalisierung der Datenbearbeitungen hinterher. Der Schwerpunkt der internationalen Zusammenarbeit liegt gegenwärtig beim gegenseitigen Informationsaustausch; noch ausbaubedürftig ist hingegen die Arbeitsteilung und Koordination bei der Entwicklung konkreter Normen und der Aufsichtstätigkeit. Soweit aufgrund der wenigen im Rahmen der Evaluation hierzu gemachten Abklärungen überhaupt eine sehr vorläufige Schlussfolgerung möglich ist, erscheint die Arbeitsteilung mit den kantonalen Datenschutzbeauftragten im Sinne einer einheitlichen Rechtsinterpretation für die Bearbeiter grundsätzlich als sinnvoll. Die Zusammenarbeit mit den Datenschutzberatern der Departemente und Bundesämter ist unterschiedlich gut, auch ist die Bedeutung der Datenschutzberater nach Einschätzung der Interviewpartner beim EDÖB nicht überall gleich gross. Oft scheinen insbesondere in Bezug auf die Beratung der Bundesverwaltung durch den EDÖB noch immer unterschiedliche gegenseitige Rollenerwartungen zu bestehen. Insgesamt positiv bewertet werden die vom EDÖB auf Forderungen aus der Bundesverwaltung hin gemeinsam mit der Universität Freiburg initiierten Ausbildungsaktivitäten,

- *Zusammenarbeit mit privaten Datenschutzakteuren:* Fest bestehende Datenschutzstrukturen bestehen vermutlich nur in grossen Unternehmen oder KMU, die auf den Umgang mit sensiblen Daten spezialisiert sind. Was die gesetzlichen Neuerungen (Zertifizierung, Datenschutzverantwortliche in den Betrieben) diesbezüglich bewirken, wurde nicht evaluiert. Neu entstandene Fachvereine für betriebliche Datenschutzverantwortliche ermöglichen einen guten Austausch mit dem EDÖB. Bei potenziellen Organisationen zum Schutz der Betroffenen (vorab Konsumentenschutzorganisationen, Arbeitnehmerorganisationen, Patientenschutzorganisationen) ist der Datenschutz bislang ein wenig beachtetes Thema.

- *Doppelrolle für Datenschutz und Öffentlichkeitsprinzip:* Die Doppelrolle des EDÖB im Vollzug des DSG und des BGÖ beeinträchtigt die Wahrnehmung der datenschützerischen Aufgaben prinzipiell nicht. Da die Mehrbelastung durch die neuen Aufgaben im Bereich des BGÖ jedoch finanziell nicht vollumfänglich aufgefangen wurde, ergab sich in der Praxis eine Ressourcenschmälerung des für die Belange des Datenschutzes. Inwieweit die Aufgabenerfüllung des EDÖB für das BGÖ durch die Pflichten aus dem DSG beeinträchtigt wird, war nicht Gegenstand der Evaluation (vgl. aber Ziffer 11.2.5).

- *Ressourcen:* Im Verhältnis zu seinen vielfältigen Aufgaben ist die Ausstattung des EDÖB mit personellen Ressourcenausstattung als schwach zu beurteilen. Diese vom EDÖB vorgetragene Kritik wird auch von den befragten Rechtsexperten und Interessenvertretern (auf Seiten der Betroffenen) geteilt. Zwar sind die Personalressourcen des EDÖB von 2000 bis 2005 gewachsen. Danach haben die Mittel jedoch nur noch schwach zugenommen, und ins-

besondere ist der ursprünglich geschätzte Personalaufwand für die neuen Aufgaben im Zusammenhang mit dem BGÖ nicht aufgefangen worden. Obwohl internationalen Vergleichen aufgrund der unterschiedlichen Pflichtenhefte und Grösse der Länder enge Grenzen gesetzt sind, besteht der Eindruck, dass ausländische Datenschutzbeauftragte tendenziell über mehr Mittel als der EDÖB verfügen.

13.3 Wirksamkeit und Grenzen der Wirksamkeit des EDÖB

In diesem Abschnitt soll bilanziert werden, wie die Wirksamkeit des EDÖB für eine Verbesserung des Datenschutzes im Sinne des DSG insgesamt zu beurteilen ist, und wo die Evaluation Hinweise auf Grenzen der Wirksamkeit liefert. Der EDÖB setzt seine Ressourcen schwergewichtig für die vom DSG vorgeschriebenen Aufgaben der Aufsicht, der Beratung und der Information ein. Diese Aufgaben stehen im Zentrum der folgenden Bilanzierung zur Wirksamkeit und ihrer Grenzen; daneben berücksichtigen wir auch weitere Aspekte, die hinsichtlich der Wirksamkeit von Bedeutung sind.

13.3.1 Wirksamkeit des EDÖB

Aufsichtstätigkeit: wirksam im Einzelfall

Im Rahmen seiner Aufsichtstätigkeit kann dem EDÖB eine hohe Wirksamkeit im Einzelfall zugesprochen werden. In denjenigen Fällen, in denen der Datenschutzbeauftragte im Rahmen seiner Aufsichtstätigkeit Sachverhaltsabklärungen durchführt, kann er letztendlich sicherstellen, dass die Datenbearbeitungen gemäss dem DSG durchgeführt werden. In der Mehrheit der Fälle ergeben die Sachverhaltsabklärungen nur geringfügige Probleme, welche die Bearbeiter denn auch freiwillig beheben. Richtet der EDÖB im Anschluss an eine Sachverhaltsabklärung eine Empfehlung an einen Datenbearbeiter, wird diese in vier Fünfteln der Fälle direkt oder seltener indirekt (nach einem Gerichtsentscheid) umgesetzt. Dabei ist die Strategie des EDÖB, seine Empfehlungen konsequent auf dem Gerichtsweg zu verteidigen, wenn sie vom Bearbeiter nicht umgesetzt wird, als wirksam und essentiell für seine Glaubwürdigkeit zu beurteilen; sie hat allerdings den Preis, dass sie im Einzelfall mit einem hohen Aufwand verbunden ist (vgl. Ausführungen zur Ressourcensituation weiter unten) und dazu führt, dass insgesamt nur eine sehr beschränkte Anzahl Fälle behandelt werden kann. Empfehlungen, die auf dem Gerichtsweg nicht durchgesetzt werden können, dienen immerhin der Klärung der Rechtslage. Durch systematische Nachkontrollen stellt der EDÖB die Umsetzung der verlangten Massnahmen sicher.

Diese Wirkung im Einzelfall erzielt der EDÖB, obwohl seine Möglichkeiten zur Beschaffung der notwendigen Informationen und zur Sanktionierung von fehlbaren Bearbeitern im internationalen Vergleich eher schwach ausgestattet sind (seitens des EDÖB wünscht man sich diesbezüglich denn auch stärkere Kompetenzen). Die mit einer Empfehlung verbundene Veröffentlichung eines Missstands wird von vielen Datenbearbeitern gescheut. Die Bereitschaft zu Anpassungen seitens der Datenbearbeiter dürfte somit oft mit Imageüberlegungen zusammenhängen; dieser Wirkungszusammenhang wird vom EDÖB gut genutzt, indem er seine Beschwerden und die

Gerichtsurteile öffentlich macht, gleichzeitig aber durch eine zurückhaltende oder anonymisierte Informationstätigkeit auch Anreize zu kooperativem Verhalten setzt.

Beratungs- und Informationstätigkeit: Wirksam im Einzelfall

Die Beratungs- und Informationstätigkeit zu Gunsten privater und öffentlicher Datenbearbeiter kann für den Einzelfall ebenfalls als wirkungsvoll bezeichnet werden. Die Beratung, die im Einzelfall und auf Anfrage durchgeführt wird, wird von den Bearbeitern insgesamt als nützlich, praxisnah und konstruktiv bewertet. Abstriche machen jedoch diesbezüglich die Bundesorgane, die den EDÖB als Berater teils kaum wahrnehmen. Somit kann der EDÖB in denjenigen Einzelfällen, in denen er Datenbearbeiter direkt berät, durchaus zur Durchsetzung der Bestimmungen des DSG beitragen. Auch die Qualität der Publikationen des EDÖB beurteilen die befragten Datenbearbeiter und Experten überwiegend als gut bis sehr gut. Durch den Ausbau des Informationsangebots auf Internet konnte die Effizienz der Beratung gesteigert werden. Hinsichtlich der Informationstätigkeit lässt sich festhalten, dass die Merkblätter und Leitfäden des EDÖB gemäss den befragten Datenbearbeitern für die praktische Arbeit als nützlich empfunden werden. Der Meinung des EDÖB kommt in dieser Beziehung Gewicht zu. Zuweilen wurde der Wunsch geäussert, der EDÖB solle vermehrt derartige Dokumente zur Verfügung stellen.

Die Beratung von Betroffenen hat der EDÖB stark rationalisiert, um Ressourcen für andere Aktivitäten freizuhalten. Zum einen werden Anfragen Betroffener mit Standardbriefen beantwortet, die sie über ihre Rechte aufklären, zum anderen wurde das Informationsangebot auf der Homepage erweitert, um die Beratung zu entlasten. Dieses Vorgehen hat die Wirksamkeit der Beratung im Einzelfall möglicherweise etwas beeinträchtigt, die Effizienzsteigerung dürfte aber Mittel für andere Aktivitäten mit einer höheren Gesamtwirkung freigespielt haben und ist insofern als sinnvoll zu beurteilen.

Aus Sicht der Evaluatoren stellt sich allenfalls die Frage, ob sich die in verschiedener Hinsicht grosse Vielfalt an Beratungstätigkeiten angesichts der knappen Ressourcen rechtfertigen lässt; die insbesondere von Bundesorganen geäusserte Kritik, dass der EDÖB seine Beratungstätigkeit teilweise ungenügend wahrnehme, weist ebenfalls in diese Richtung. Dabei gilt es zu berücksichtigen, dass der EDÖB den verschiedenen Arten von Beratungen jeweils einen spezifischen Nutzen (z.B. Sicherstellung der Praxisnähe, Sensibilisierung und Kontaktpflege zu den Bearbeitern, „Problemortung“ durch die Beratung von Betroffenen) zuordnet, so dass jede Einschränkung der Beratungstätigkeit mit gewissen Folgen auch für andere Aktivitäten verbunden wäre.

13.3.2 Grenzen der Wirksamkeit

Die Evaluation zeigt demgegenüber auch Grenzen des Wirkungsmechanismus EDÖB auf, die ihre Ursachen in der Ressourcenausstattung, den technologischen Herausforderungen oder aber in den gesetzlichen Bestimmungen selber haben können.

Grenzen der Aufsichtstätigkeit bei unübersichtlichen Konstellationen

Als erstes zeigte sich, dass das Instrument der Aufsicht bei neuen Herausforderungen im Internet an seine Grenzen stossen kann. Zum einen ist hier die Wahrnehmbarkeit von Missbräuchen eingeschränkt, zum anderen der Zugriff auf die Bearbeiter. Das Beispiel der *Sozialen Netzwerke* macht deutlich, dass beim Vorliegen bestimmter Bedingungen die Wirksamkeit des DSG eingeschränkt ist. Dies ist insbesondere dann der Fall, wenn der Datenbearbeiter seinen Sitz im Ausland hat. Hinzu kommt bei Datenbearbeitungen mit neuen Technologien auf Basis des Internets, dass die Betroffenen selber persönliche Informationen auf ihrem Profil veröffentlichen oder bisweilen gar nicht Kenntnis darüber haben (können), wer welche Daten von ihnen bearbeitet. In diesem Fall können sie auch den EDÖB nicht informieren. Ebenfalls stellt die quantitative Zunahme neuer Anwendungen im Internet im Zuge der technologischen Entwicklung eine Herausforderung dar, die auch angesichts der Ressourcensituation beim EDÖB als problematisch eingestuft werden muss.

Wenn der Zugriff auf den Bearbeiter erschwert ist, weil dieser vom Ausland her operiert, kann internationale Koordination der Datenschutzbehörden gelegentlich eine Erfolg versprechende Gegenstrategie sein. Diesbezüglich ist der Fall *Logistep* illustrativ. Der Entscheid des EDÖB, gegen den in der Schweiz ansässigen, aber international aktiven Datenbearbeiter vorzugehen, wurde ausgelöst durch ausländische Datenschutzbehörden. Allerdings ist es dem betreffenden Anbieter prinzipiell möglich, seine Dienste nun von einem anderen Land mit weniger restriktiver Praxis anzubieten. Beide Fälle (*Soziale Netzwerke, Logistep*) verweisen somit auf die Notwendigkeit internationaler Absprachen unter den Datenschutzbehörden.

Dass auf die Bearbeiter keine Zugriffsmöglichkeit besteht, trifft jedoch nicht für alle neuartigen Anwendungen zu: Auch im Internetbereich gibt es Beispiele, die von der Ausgangslage her klassischen Konstellationen ähneln und entsprechend der Aufsichtstätigkeit durch den EDÖB zugänglich sind. Es gibt eine Reihe von Beispielen (vgl. z.B. die Fallstudien *Mitarbeitercheck* und *Logistep*), in denen sich der EDÖB wirksam mit neuen Produkten und Dienstleistungen im Netz auseinandergesetzt hat. Zu beachten gilt es dabei allerdings, dass es aufgrund der technologischen Entwicklungen heute relativ einfach geworden ist, Dienstleistungen im Internet aufzuschalten, was sich auch in der grossen Zahl solcher Angebote zeigt. Diese Mengenausweitung dürfte sich in Zukunft fortsetzen. Hier stellt sich die Frage, inwieweit der EDÖB den Herausforderungen angesichts der knappen Ressourcen gerecht werden kann.

Begrenzte Inanspruchnahme der Beratung aufgrund der Doppelrolle des EDÖB

Die Wirksamkeit der Beratung zugunsten privater und öffentlicher Datenbearbeiter hinsichtlich korrekter Datenbearbeitungen ist insofern begrenzt, als der EDÖB von einem Teil der Bearbeiter aufgrund seiner Doppelrolle als Aufsichts- und Beratungsorgan gemieden wird; auch kann er Bearbeiter nicht mit der Möglichkeit ködern, ihnen im Rahmen einer vorgängigen Prüfung ihrer Projekte eine Garantie auszusprechen und dadurch das Investitionsrisiko zu minimieren. In dieser Hinsicht ist somit fraglich, ob mit der Beratungstätigkeit tatsächlich auch besonders problematische Datenbearbeitungen abgedeckt werden, oder ob sich die Beratung unter den gegebenen

gesetzlichen Bedingungen nicht primär auf Datenbearbeitungen bereits sensibilisierter Datenbearbeiter mit einem eher geringen Gefährdungspotenzial bezieht.[254]

Begrenzte resp. unklare Resonanz der Publikationen – nicht messbarer Sensibilisierungseffekt

In Fällen, in denen keine Sachverhaltsabklärungen durchgeführt werden können, hat der EDÖB die Möglichkeit, mit Hilfe von Publikationen zum Thema die Betroffenen und allenfalls die Bearbeiter sachgerecht über Möglichkeiten des Selbstschutzes zu informieren und auf problematische Praktiken hinzuweisen. Inwieweit die Beiträge des EDÖB auf seiner Homepage von den Betroffenen konsultiert werden, oder gar welche Wirkungen sich daraus ergeben, konnte im Rahmen der Evaluation nicht eruiert werden. Die Internetseite des EDÖB wird zwar recht gut frequentiert und als nützlich beurteilt. Die Nutzungsstatistik, die Ergebnisse der Bevölkerungsbefragung und Einschätzungen von Experten wecken gleichwohl keine allzu grossen Hoffnungen, dass durch die blosse Publikation bestimmter Inhalte auf der Homepage und im Tätigkeitsbericht direkt breite Bevölkerungsschichten angesprochen und sensibilisiert werden können.

Zentral für die Präsenz seiner Äusserungen in der Öffentlichkeit und den Zielgruppen ist es, dass der EDÖB andere Akteure für seine Anliegen als Hebel einsetzen kann. Relativ häufig gelingt dies via Medien: Der EDÖB ist in den dort präsent und bemüht sich im Rahmen seiner Möglichkeiten ausreichend, seine Stellungnahmen bekannt zu machen. Allerdings wird die öffentliche Resonanz eines Themas nicht vom EDÖB, sondern von den Medien definiert. Eher selten kann er seine Informationen auch in die Kommunikationsmassnahmen anderer Bundesorgane integrieren, wie das im Bereich „Jugend und Internet“ glückte.

Begrenzte Wirksamkeit der Stellungnahmen in Rechtsetzungsprozessen

Die verfügbaren Informationen zur Umsetzung der Stellungnahmen des EDÖB zu Vorlagen über Erlasse und Massnahmen des Bundes lassen nur provisorische Schätzungen der Wirksamkeit des EDÖB zu. Festgehalten werden kann, dass der EDÖB über die Vorlagen in aller Regel informiert ist und Gelegenheit zur Stellungnahme erhält und diese in der Regel in den amtlichen Berichten zu den Konsultationsverfahren ersichtlich ist. Wenn dies nicht der Fall ist, versucht er sich später im Entscheidungsprozess einzubringen. Insofern ist die Mindesterwartung des Gesetzes erfüllt. Der EDÖB selbst schätzt, dass seine Verbesserungsvorschläge in der Minderheit der Fälle gar nicht und ansonsten teilweise – was häufig der Fall ist – oder vollständig berücksichtigt werden.

Begrenzte Wirksamkeit der Registrierpflicht und der Bearbeitungsreglemente

Bezüglich der Registrierpflicht und der daran anschliessenden Verpflichtung zur Erstellung von Bearbeitungsreglementen ist das Fazit durchzogen. Es ist nicht auszuschliessen, dass viele Daten-

[254] Die Beratung im Fall *SAKE*, welche im Nachgang zu Sachverhaltsabklärungen führte, ist hierfür kein Gegenbeispiel. Sie wurde nicht vom bearbeitenden Bundesamt gesucht, sondern vom EDÖB nach Hinweisen in den Medien und seitens der Betroffenen initiiert.

sammlungen nicht im Register eingetragen sind, und dass viele Bearbeitungsreglemente gar nicht bestehen oder nur mangelhaft ausgestaltet sind. Daraus folgt die Vermutung, dass die damit bezweckten Wirkungen (Transparenz für die Bevölkerung, Sensibilisierung der Datenbearbeiter) nur teilweise erreicht werden.

Ressourcen als Grenze der Wirksamkeit im Einzelfall

Aufgrund der Ressourcensituation des EDÖB ist davon auszugehen, dass er seine Aufsichts- und Beratungsfunktion umfassender – das heisst – in mehr Fällen vornehmen könnte, wenn er mehr Mittel dazu hätte. So gibt der EDÖB an, dass Fälle teils aus Ressourcengründen nicht oder nicht sofort bearbeitet werden können, obschon eine Bewertung nach den üblichen Kriterien dies rechtfertigen würde. Der Weiterzug von Empfehlungen kann sich als besonders ressourcenintensiv erweisen und beträchtliche Mittel an den jeweiligen Fall binden. Auch die Kontrolle der Registrierpflicht und der Existenz der teils obligatorischen Bearbeitungsreglemente kann mit den bestehenden Ressourcen nicht flächendeckend sichergestellt werden.

Orientierung an der öffentlichen Resonanz als mögliche Grenze der Wirksamkeit

Der EDÖB orientiert seine Aktivitäten stark an den Inputs, mit denen er aufgrund von Anfragen von Betroffenen und Bearbeitern, der öffentlichen Debatte und der internationalen Fachdiskussion konfrontiert ist. Da er insbesondere bei Fällen, über die bereits eine öffentliche Debatte im Gange ist, eine grosse Resonanz erzielen kann, besteht für ihn ein Anreiz, diese Fälle privilegiert zu behandeln. Es besteht dabei ein latentes Risiko, dass dabei Praktiken, die insgesamt ein grösseres Gefahrenpotenzial für die Privatheit der Betroffenen bergen, weniger Beachtung finden. Im Bereich der Bundesorgane ist der EDÖB aufgrund des Legalitätsprinzips und seiner regelmässigen Konsultation im Rahmen von Vorlagen des Bundesrats umfassender über die beabsichtigten Datenbearbeitungen informiert und kann deshalb seine Schwerpunkte gezielter setzen.

Begrenzte resp. unklare Wirkung der Aufsicht über den Einzelfall hinaus

Eine weitere Grenze der Wirksamkeit zeigt sich bei der Aufsicht, wenn nach den Wirkungen über den Einzelfall hinaus gefragt wird. Der EDÖB kann aufgrund seiner Ressourcensituation keine flächendeckenden Kontrollen in einer ganzen Branche durchzuführen. Stellt der EDÖB im Rahmen einer Sachverhaltsabklärung Datenbearbeitungen fest, die seiner Ansicht nach nicht im Einklang mit dem DSG stehen, so sieht er sich heute nicht in der Lage, bei weiteren Anbietern, die ähnliche Bearbeitungen durchführen, sicherzustellen, dass das DSG eingehalten wird. Schon Stichproben würden gemäss seinen Aussagen so viele Ressourcen binden, dass er in anderen Fällen nicht aktiv werden könnte. Das einzige Mittel, das ihm bleibt, ist somit in der Regel die öffentliche Information. Ausnahmsweise ist es schon vorgekommen, dass der EDÖB gezielt auf die betreffende Branche zuging.

Eine präventive Wirkung auf andere Datenbearbeiter entsteht somit am ehesten dort, wo eine Sachverhaltsabklärung auf ein öffentliches Interesse stösst und entsprechend in den Medien por-

tiert werden kann; die damit einhergehende Sensibilisierung für die Problematik kann Betroffene zu Beschwerden motivieren und Bearbeiter aufgrund des drohenden Image-Schadens dazu bewegen, sich an die Vorschriften zu halten, indem die Datenbearbeitung angepasst oder eingestellt wird. Es bleibt jedoch im Rahmen dieser Evaluation unklar, inwiefern von derartigen Publikationen allein tatsächlich eine Breitenwirkung, also ein Lerneffekt bei anderen Bearbeitern ausgeht. Hierzu können keine empirisch fundierten Aussagen gemacht werden.

13.4 Gesamtbilanz

Insgesamt kann bilanziert werden, dass der EDÖB seinen gesetzlichen Auftrag erfüllt und im Rahmen seiner Möglichkeiten eine hohe Wirksamkeit erzielt. Er verfügt über eine seinem Auftrag und seinen Ressourcen insgesamt angemessene Organisation und Strategie. Es sind primär von ihm nicht beeinflussbare Rahmenbedingungen, die seiner Wirksamkeit Grenzen setzen. Diese sind zum Teil politisch gewollt, wie die Ressourcenausstattung und der gesetzliche Rahmen, der seine Pflichten und Möglichkeiten definiert. Zum Teil stehen diese Grenzen jedoch nicht zur Disposition der (schweizerischen) Politik, so die zunehmende Internationalisierung der Datenbearbeitung, die sinkende Transparenz der Datenbearbeitungen und die Themensetzung der öffentlichen Diskussion.

Die Grenzen der Wirksamkeit führen dazu, dass Datenbearbeiter vieler Branchen nicht damit rechnen müssen, bei datenschutzrechtlich heiklen oder gar illegalen Praktiken eine Sachverhaltsabklärung mit entsprechenden Folgen zu riskieren. Dieser zusammenfassende Befund gilt gemäss den Erkenntnissen dieser Evaluation vermutlich auch für die gesetzliche Verpflichtung der Bearbeiter, ihre Datensammlungen im öffentlichen Register anzumelden und Bearbeitungsreglemente zu erstellen. Inwieweit die Meldepflicht für Datenbekanntgaben ins Ausland eingehalten wird, wurde nicht untersucht.

TEIL V: SYNTHESE

Der Gegenstand der vorangehenden Berichtsteile war die Evaluation des schweizerischen Datenschutzgesetzes (DSG). Dieses bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Das der Evaluation zugrunde liegende Wirkungsmodell basiert auf der Annahme, dass für die Beziehung zwischen Betroffenen und Datenbearbeitern die Sensibilität für Datenschutzfragen beider Akteursgruppen entscheidend ist. Sensibilisierte Betroffene versuchen sich soweit als möglich selbst vor missbräuchlichen Datenbearbeitungen zu schützen. Sensibilisierte Bearbeiter wiederum räumen datenschutzrechtlichen Belangen bei der Verfolgung ihrer Ziele ein gebührendes Gewicht ein und halten die gesetzlichen Bestimmungen ein. Diese Sensibilität der Akteure wiederum hängt von den Rahmenbedingungen ab, die sich über die Zeit wandeln können, insbesondere von der technologischen Entwicklung. Einen wichtigen Hintergrund der Evaluation bildet denn auch die Tatsache, dass sich seit dem Inkrafttreten des DSG am 1. Juli 1993 die Informations- und Kommunikationstechnologien stark entwickelt und neue Anwendungen rege genutzt werden, das Gesetz bisher jedoch nur punktuell revidiert worden ist.

Das DSG greift mit zwei Wirkungsmechanismen in die Beziehung zwischen den Datenbearbeitern und den betroffenen Personen ein. Erstens setzt der Gesetzgeber auf die Eigenverantwortung und gibt den Betroffenen Rechte in die Hand, mit denen sie die Einhaltung der Grundsätze des DSG vor Gericht durchsetzen können (Wirkungsmechanismus der Durchsetzungsrechte). Zweitens setzt der Gesetzgeber auf eine unabhängige staatliche Behörde, der er die Aufsicht über die Bearbeiter sowie die Beratung und Information der Bearbeiter und der Betroffenen übertragen hat (Wirkungsmechanismus des EDÖB).

Der folgende Teil bildet die Synthese des Berichts. Dabei wird in Kapitel 14 aus übergeordneter Perspektive Bilanz über die Befunde der Evaluation gezogen. Zunächst wird in einem kurzen Abschnitt auf einige Unterschiede eingegangen, die sich bezüglich privaten Datenbearbeitern und Bundesorganen in der Evaluation ergeben haben. In einem zweiten Schritt werden die festgestellten Wirkungen des DSG, um sie besser einordnen zu können, in Bezug zu verschiedenen Referenzgrössen gesetzt. Basierend auf den Befunden zu den Aktivitäten des EDÖB werden danach in Kapitel 15 zunächst einzelne *praktische Empfehlungen* an den EDÖB hergeleitet. Weiter werden – ohne Anspruch auf Vollständigkeit – *weiterreichende Handlungsoptionen* im Sinne von Gedankenanstössen skizziert. Diese fussen einerseits in den Befunden der Evaluation und sind andererseits inspiriert von den gegenwärtigen datenschutzrechtlichen Reformbestrebungen auf europäischer Ebene, die in Kapitel 15 ebenfalls kurz vorgestellt werden.

Es wird im Rahmen dieser Synthese darauf verzichtet, die Ergebnisse der Evaluation ausführlich zusammenzufassen. Hierfür sei auf die *Zusammenfassung am Anfang des Berichts* sowie auf die jeweiligen *Fazit-Kapitel am Ende der Teile II, III und IV* dieser Evaluation verwiesen: Kapitel 6 behandelt dabei zusammenfassend die technologischen Entwicklungen und ihre Folgen für den Datenschutz sowie die Sensibilität der Datenbearbeiter und der Betroffenen. Kapitel 10 geht auf die Inanspruchnahme der Durchsetzungsrechte und auf die Rechtsprechung der Gerichte ein. Kapitel 13 behandelt organisatorische Aspekte und die Wirksamkeit des EDÖB.

14 Bilanz der empirischen Befunde

In diesem Kapitel wird aus übergeordneter Perspektive Bilanz über die Befunde der Evaluation gezogen. Zunächst wird in einem kurzen Abschnitt auf einige Unterschiede eingegangen, die sich bezüglich privater Datenbearbeiter und Bundesorgane in der Evaluation ergeben haben. In einem zweiten Schritt werden die festgestellten Wirkungen des DSG, um sie besser einordnen zu können, in Bezug zu verschiedenen Referenzgrössen gesetzt. Es wird dabei gefragt, ob erstens das aktuell durch das DSG gewährleistete Niveau des Datenschutzes dem Niveau entspricht, das bei Inkrafttreten des Gesetzes erwartet wurde, inwieweit zweitens das Gesetz den Erwartungen der Bevölkerung und der Bearbeiter entspricht und wie ausgebaut drittens die Instrumente des Datenschutzgesetzes im internationalen Rechtsvergleich sind; viertens soll auch die Frage angesprochen werden, ob das DSG den grundrechtlichen Schutz der Persönlichkeit nach Art. 13 Abs. 2 BV garantieren kann. Diese Fragen können nicht abschliessend beantwortet werden, gleichwohl sind Hinweise möglich, die es erlauben, die Wirkungen des DSG besser einordnen zu können.

14.1 Bearbeitungen durch Private und Bundesorgane im Vergleich

Differenziert man bezüglich den auf die Bearbeiter wirkenden gesetzlichen Bestimmungen des DSG sowie weiteren, nicht gesetzliche Faktoren zwischen Bundesorganen und privaten Bearbeitern, so lassen sich verschiedene Unterschiede feststellen:

- *Anreize zu datenschutzkonformem Verhalten:* Insgesamt wurden sowohl zwischen den Bundesorganen wie auch zwischen privaten Bearbeitern Unterschiede hinsichtlich ihrer Sensibilität den Datenschutz festgestellt. Anreizstrukturen für ein gesetzeskonformes Verhalten bestehen für beide Gruppen, doch unterscheiden sich die Mechanismen für private und öffentliche Bearbeiter leicht. Die von den privaten Bearbeitern vermutete Sensibilität der Betroffenen führt dazu, dass die Bearbeiter offensichtliche DSG-Verstösse teils aus Imagegründen vermeiden oder diese bei deren Aufdeckung korrigieren, um negative Folgen am Markt zu vermeiden. Für Bundesorgane bildet demgegenüber ein vermuteter Vertrauensverlust der Bürgerinnen und Bürger einen Anreiz, die Bestimmungen des DSG einzuhalten. Die Folge eines Vertrauensverlustes kann z.B. eine geringere Auskunftsbereitschaft der Bürgerinnen und Bürger und damit verbunden eine geringere Datenqualität sein.

- *Folgen der technologischen Entwicklung:* Die Folgen der technologischen Entwicklung für den Datenschutz lassen sich anhand dreier Trends beschreiben, die hinsichtlich der Bearbeitungen durch Bundesorgane und Private von unterschiedlicher Bedeutung sind. Erstens ist eine mengenmässige Zunahme an Datenbearbeitungen festzustellen. Diese Mengenausweitung der Datenbearbeitungen betrifft den öffentlichen und den privaten Sektor. Zweitens wurde festgestellt, dass insbesondere bei internetbasierten Datenbearbeitungen häufig Intransparenz sowohl über den Bearbeiter als auch über die Bearbeitung an sich besteht. Derartig intransparente Bearbeitungen sind primär im Privatsektor anzutreffen, da im öffentlichen Sektor das Erfordernis der gesetzlichen Grundlage (Art. 17 Abs. 1 DSG) für eine gewisse Transparenz gegenüber der Öffentlichkeit sorgt, und der Bearbeiter somit meist identi-

fizierbar sein dürfte. Als dritter Trend zeigte sich, dass die Bearbeitung der Daten von Personen in der Schweiz zunehmend grenzüberschreitend vom Ausland her erfolgt, und sich solche Bearbeiter damit dem rechtlichen Zugriff entziehen. Bearbeiter mit Sitz im Ausland können per Definition keine Bundesorgane sein, dieser Trend betrifft somit nur den Privatsektor.

- *Durchsetzungsrechte:* Der Gerichtsweg wird von den Betroffenen im Zusammenhang mit Datenbearbeitungen durch Bundesorgane – im Vergleich mit dem Privatbereich – häufiger, wenn auch absolut gesehen immer noch selten beansprucht. Dieser Unterschied gilt sowohl für das Recht auf Auskunft (Art. 8 DSG), das insgesamt etwas häufiger beansprucht wird, als auch für die Durchsetzungsrechte auf Berichtigung, Sperrung, Vernichtung und Vermerkung von Daten (Art. 15 bzw. Art. 25 DSG). Eine mögliche Teilerklärung für diese Diskrepanz dürfte in der Tatsache liegen, dass intransparente Bearbeitungen und Bearbeitungen vom Ausland her in stärkerem Ausmass den Privatsektor betreffen als den öffentlichen Sektor.

- *Dienstleistungen des EDÖB:* Naturgemäss erwarten sowohl private Datenbearbeiter als auch Bundesorgane vom EDÖB primär Informations- und Beratungsleistungen. Die bestehenden Probleme sind jedoch unterschiedlich gelagert. Während private Bearbeiter bisweilen den EDÖB meiden, weil dieser gleichzeitig Aufsichtsorgan ist, kommt bei den Bundesorganen der Wunsch nach einer Ausweitung der Beratungstätigkeit deutlich zum Ausdruck.

- *EDÖB – Breitenwirkung einzelner Aktivitäten:* Es wurde festgestellt, dass der EDÖB nach Sachverhaltsabklärungen bei einzelnen Bearbeitern bei gleichartigen Unternehmen nicht kontrolliert, ob diese sich an seine Handlungsanweisungen halten. Bei öffentlichen Bearbeitern stellt sich diese Frage der so erzielbaren Breitenwirkung der Aufsichtstätigkeit weniger dringend, geht es doch häufig um Anwendungen, die in dieser Form nur von einem einzelnen Akteur – eben dem betreffenden Bundesorgan – betrieben werden. Bei Privaten kommt es hingegen häufiger vor, dass vom EDÖB Empfehlungen, aber auch Leitfäden und Merkblätter als „Standards" für eine ganze Branche Geltung beanspruchen, ohne dass der EDÖB deren Einhaltung umfassend prüfen kann.

- *Rechtsgrundlage der Datenbearbeitung:* Hinsichtlich der rechtlichen Erfordernisse für Datenbearbeitungen besteht zwischen Bundesorganen und privaten Bearbeitern ein wesentlicher Unterschied, dürfen doch erstere Daten nur bei Vorliegen einer hinreichenden gesetzlichen Grundlage bearbeiten. Zunächst sorgt dieser Grundsatz für Bundesorgane für Transparenz. Die Öffentlichkeit und der EDÖB sind insbesondere bei geplanten Bearbeitungen besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen durch Bundesorgane schon im Voraus besser informiert als bei Bearbeitungen privater Akteure. Gleichzeitig bestehen aufgrund des formalisierten Planungs- und Gesetzgebungsprozesses interne Kontrollen sowie Interventionsmöglichkeiten für den EDÖB und andere am Datenschutz interessierte Kreise, die bei neuen Anwendungen von Privaten nicht zwingend vorgesehen sind. Umgekehrt stellt sich die Frage, ob nicht die Gefahr besteht, dass eine demokratisch legitimierte Datenbearbeitung den vom DSG vorgesehenen und sogar den in der Verfassung verankerten Minimalschutz potenziell aushebelt. Dieser Aspekt wird nachstehend nochmals aufzugreifen sein (vgl. Ziffer 14.2.4).

14.2 Wirksamkeit des Gesetzes in Bezug auf verschiedene Referenzgrössen

Die empirische Untersuchung des Datenschutzgesetzes zeigt, dass dieses wohl Wirkungen in der beabsichtigten Richtung erzielt hat, und dass diese Wirkungen teils von Marktmechanismen unterstützt werden. Gleichzeitig zeigt sich aber auch, dass die Wirkungen begrenzt sind – nicht nur, aber auch aufgrund der mit der technologischen Entwicklung verbundenen neuen Herausforderungen. Der Selbstschutz durch die Betroffenen stösst an Grenzen, weil es für sie schwieriger geworden ist, den Überblick über die eigenen Daten zu behalten. Der Wirkungsmechanismus des Rechtswegs hat sich als insgesamt wenig genutzter Pfad zur Durchsetzung der Datenschutzgrundsätze erwiesen. Die Aktivitäten des Eidgenössischen Datenschutz- und Öffentlichbeauftragten zeitigen zwar Wirkungen, doch stossen auch sie an gewisse äussere Grenzen.

Eine zentrale Frage an die Evaluation ist, ob die gesetzlichen Bestimmungen des DSG geeignet sind, einen angemessenen Schutz der Persönlichkeit für Personen, über die Daten bearbeitet werden, zu gewährleisten. Ob das hier anhand der gemachten Befunde grob abschätzbare Schutzniveau *angemessen* ist, ist jedoch aus den rechtlichen Grundlagen nicht direkt abzuleiten, da der vom Gesetz angestrebte Sollzustand nicht präzis umschrieben wird. Der Gesetzgeber hat keine messbaren Ziele definiert, die mit dem DSG erreicht werden sollen. Die einzige rechtliche Messlatte des Gesetzes sind prinzipiell die Einhaltung der Datenschutzgrundsätze nach Art. 4 DSG, wobei diese Werte im konkreten Fall mit den Interessen der Bearbeiter abgewogen werden müssen. Als Minimalstandard gilt der durch Art. 13 Abs. 2 BV und Art. 8 EMRK definierte, aber ebenfalls auslegungsbedürftige Anspruch auf den Schutz vor Missbrauch der persönlichen Daten und die Wahrung der informationellen Selbstbestimmung.

Das anzustrebende Schutzniveau ergibt sich somit nicht ohne weiteres, weshalb nachfolgend mehrere Referenzgrössen herangezogen werden, *um die Schutzwirkungen des DSG, wie sie im Rahmen dieser Evaluation festgestellt wurden, besser einordnen zu können.* Ob das hier festgestellte Schutzniveau angemessen ist, ist schlussendlich auch eine politische Frage, die somit in dieser Evaluation nicht abschliessend zu beantworten ist.

Als behelfsmässige Referenzgrössen zur Einordnung der aktuellen Wirksamkeit des Gesetzes werden im Folgenden erstens die Erwartungen zum Zeitpunkt des Inkrafttretens des DSG im Jahre 1993 herangezogen. Zweitens werden die Wirkungen mit den Einstellungen und Erwartungen der Bürgerinnen und Bürger sowie der Datenbearbeiter zum Datenschutz und zum DSG verglichen. Aus rechtlicher Perspektive wird als dritter Referenzpunkt die Datenschutzgesetzgebung anderer westlicher Länder herangezogen, und viertens sind institutionelle Hindernisse zu thematisieren, die der Garantie des verfassungsmässig vorgesehenen Mindestniveaus des Persönlichkeitsschutzes Grenzen setzen.

14.2.1 Referenzgrösse 1: Beabsichtigtes Schutzniveau zum Zeitpunkt des Inkrafttretens

Das schweizerische Datenschutzgesetz ist 1993 in Kraft getreten und war somit zu diesem Zeitpunkt die politisch mehrheitsfähige Antwort auf die damaligen Herausforderungen des Datenschutzes durch die technische, wirtschaftliche und gesellschaftliche Entwicklung. Insofern kann das damals durch den Gesetzgeber beabsichtigte Schutzniveau als demokratisch legitimierter Soll-

Zustand und Massstab herangezogen werden. Damit stellt sich erstens die Frage, ob das Gesetz in Bezug auf die 1993 bestehenden Herausforderungen die beabsichtigte Schutzwirkung erreicht hat. Zweitens ist zu fragen, ob das Gesetz und die Umsetzungsakteure in der Lage waren, das Schutzniveau auf Dauer aufrecht zu erhalten. Veränderungen im Schutzniveau können sich dabei aus Veränderungen des Umfelds sowie aus Veränderungen des Gesetzes und seinem Vollzug ergeben haben.

Erwartungen ins DSG bei Inkrafttreten teilweise erfüllt

Die Bestandesaufnahme der vorliegenden Evaluation zeigt eine Sensibilität der Betroffenen für den Datenschutz, welche missbräuchliche Datenbearbeitungen für Datenbearbeiter als Imagerisiko erscheinen lässt. Dies begünstigt die Sensibilität der hier ansässigen Datenbearbeiter. Das DSG hat zu dieser Sensibilisierung beigetragen – wie stark, kann aber kaum abgeschätzt werden. Auch eine direkte Wirkung des DSG auf die Bearbeiter ist feststellbar, wenn auch ebenfalls nicht zu quantifizieren.

Die Schutzwirkung des DSG entfaltet sich primär über die Aktivitäten des Datenschutzbeauftragten. Der im Gesetz angelegte Wirkungsmechanismus der Durchsetzungsrechte hat sich jedoch nur schwach auf das allgemeine Schutzniveau ausgewirkt, da er zumindest im Privatbereich faktisch kaum zur Entfaltung kam. Während also die bei Inkrafttreten des Gesetzes gehegten Erwartungen in den Wirkungsmechanismus des EDÖB tendenziell erfüllt worden sind, gilt dies kaum für den Mechanismus der Durchsetzungsrechte. Inwieweit die damaligen Erwartungen ans Gesetz auch heute noch massgeblich sind, ist eine offene Frage, die hier nicht beantwortet werden kann.

Seither eingetretene Veränderungen

Wie beschrieben, hat sich das Umfeld des Gesetzes markant verändert und den Datenschutz herausgefordert. Zu beobachten sind eine Mengenausweitung der Datenbearbeitungen, eine immer häufiger auftretende Intransparenz über die Bearbeitungen und den Bearbeiter und zunehmend Bearbeiter, die grenzüberschreitend operieren. Ein Ende dieser Entwicklungen ist nicht abzusehen. Demgegenüber hat sich das DSG mit Ausnahme einiger punktueller Reformen in seinen Grundzügen nicht verändert. In Bezug auf die Umsetzung des Gesetzes ist eine Ressourcenausweitung des EDÖB festzustellen.

Insgesamt konnten jedoch die Herausforderungen durch das veränderte Umfeld durch die Anpassungen im Gesetz und beim Vollzug nicht wettgemacht werden. Dies ergibt sich aus zwei Gründen: Erstens haben die zunehmenden Ressourcen, welche dem EDÖB zur Verfügung stehen, vermutlich mit der Mengenausweitung der Bearbeitungen nicht Schritt gehalten. Zweitens wirkt das DSG primär bei den herkömmlichen, inländischen und prinzipiell gut erkennbaren Datenbearbeitungen. Die Trends zu intransparenten und grenzüberschreitenden Bearbeitungen, die insbesondere die Grundsätze der Zweckbindung und der Erkennbarkeit tangieren dürften, entziehen sich jedoch abgesehen von den Sensibilisierungsaktivitäten des EDÖB den Wirkungsmechanismen des Gesetzes weitgehend; die Bevölkerung ihrerseits dürfte mit dem Selbstschutz ge-

rade bei neuen Technologien partiell überfordert sein oder deren Risiken tendenziell unterschätzen.

Fazit: Neue Herausforderungen nicht vollumfänglich aufgefangen

Das DSG hat zwar im Bereich der schon 1993 bestehenden Herausforderungen eine spürbare Schutzwirkung erzielt. Die Befunde der Evaluation deuten jedoch darauf hin, dass das Schutzniveau wohl angesichts der gewachsenen Herausforderungen zumindest seit einigen Jahren wieder sinkt. Zudem lässt die Tatsache, dass der Wirkungsmechanismus der Durchsetzungsrechte kaum beansprucht wird, vermuten, dass diesbezüglich die erwartete Wirkung des Gesetzes nicht erreicht werden konnte.

14.2.2 Referenzgrösse 2: Einstellungen der Bearbeiter und der Betroffenen

In diesem Abschnitt werden die Wirkungen des Gesetzes mit den Erwartungen und Einstellungen der von Datenbearbeitungen betroffenen Personen und der Datenbearbeiter in Beziehung gesetzt.

Bearbeiter

Ein umfassendes Bild von den Erwartungen und Einstellungen der Bearbeiter in Bezug auf das Datenschutzgesetz kann aufgrund der vorhandenen Daten nicht gezeichnet werden. Es kann insgesamt festgehalten werden, dass bei jenen Unternehmen in der Schweiz, die Daten von vielen Personen und/oder besonders sensible Personendaten bearbeiten, ein Bewusstsein für die Anforderungen des Datenschutzes und der Bedürfnisse der Betroffenen nach Privatheit vorhanden ist.

Das heute bestehende Datenschutzgesetz sowie der Vollzug durch den EDÖB werden heute von den befragten Datenbearbeitern insgesamt als vergleichsweise praxisnah wahrgenommen. Die durch den EDÖB erbrachten Dienstleistungen werden im Allgemeinen als gut bewertet, seine Grundhaltung als recht praxisnah. Kritisch beurteilt werden formale Verpflichtungen wie etwa die obligatorische Registrierung. Insgesamt kann davon ausgegangen werden, dass die Datenbearbeiter mit dem Status quo des aktuellen DSG gut leben können. Naturgemäss sind sie eher an den Beratungs- und Informationsleistungen des EDÖB interessiert, als an seiner Aufsichtstätigkeit. Sofern sie Erwartungen gegenüber dem DSG hegen, sind diese weitgehend erfüllt.

Betroffene

In der repräsentativen Bevölkerungsumfrage bewertet die grosse Mehrheit der Befragten die neuen Möglichkeiten des Informationsaustauschs, welche die technologische Entwicklung hervorgebracht hat, positiv und nutzt diese – wenn auch in unterschiedlichem Ausmass. Gleichzeitig zeigen die Antworten, dass die Art und Weise, wie persönliche Informationen bearbeitet werden, für breite Teile der Befragten wichtig ist. Insofern kann auf ganz allgemeiner Ebene gefolgert wer-

den, dass die Zielsetzung des DSG und von Art. 13 Abs. 2 BV, die Persönlichkeit und die Grundrechte zu schützen, durchaus dem Willen der Bevölkerung entspricht. Auch im Sinne der Bevölkerung ist die Absicht des Gesetzgebers, mit dem DSG Datenbearbeitungen nicht einfach zu unterbinden; vielmehr sollten diese so ausgestalten werden, dass der informationellen Selbstbestimmung Genüge getan wird (Bundesrat/BBl 1988 II 417-418). Mit dieser dem DSG zugrunde gelegten Konzeption hat der Gesetzgeber somit die Grundhaltung der Betroffenen gut getroffen.

Die Bevölkerungsbefragung und die Expertenaussagen deuten darauf hin, dass dem Selbstschutz Grenzen gesetzt sind, dürfte doch ein bedeutender Teil der Betroffenen weder in der Lage noch willens sein, sich selbst vor widerrechtlichen Datenbearbeitungen zu schützen. Insofern erscheint es folgerichtig, dass eine grosse Mehrheit der Bevölkerung eine unabhängige Stelle, „die zum Rechten schaut", als notwendig erachtet. Inwieweit die aktuelle Aufsichtsbehörde den Erwartungen der Betroffenen zu genügen vermag, wurde nicht eruiert.

Fazit: Ausrichtung des DSG entspricht den Erwartungen der Akteure

Zusammenfassend kann festgehalten werden, dass die Stossrichtung des DSG die Grundhaltung der Bevölkerung aufnimmt: Diese möchte an der Informationsgesellschaft teilnehmen, macht sich dabei aber über die Sicherheit ihrer persönlichen Daten Sorgen und möchte sich deshalb einer unabhängigen Stelle anvertrauen können, die sie schützt. Während seitens der Bearbeiter eher auf die Beratungstätigkeit des EDÖB gesetzt wird, erwartet die Bevölkerung durchaus, dass dieser seine Aufsichtsrolle wahrnimmt.

14.2.3 Referenzgrösse 3: Das DSG im internationalen Rechtsvergleich

Vergleicht man das schweizerische Datenschutzgesetz mit den Regelungen anderer westlicher Länder, wie dies im Rahmen dieser Evaluation vom SIR (2010) unternommen wurde, so kommt man je nach beleuchtetem Aspekt zu unterschiedlichen Urteilen.

Grundsätze und Durchsetzungsrechte: gute Ausstattung

Die Grundsätze des DSG haben eine hohe Übereinstimmung mit den Grundsätzen in anderen Ländern; der internationale Vergleich fördert diesbezüglich keine grösseren Unterschiede zu Tage. Als auffälligste Abweichung kann das Widerspruchsrecht erwähnt werden, das im deutschen Datenschutzgesetz verankert ist; es wird im Rahmen der Handlungsoptionen im folgenden Kapitel 15 diskutiert.

Im Bereich der Durchsetzungsrechte, die von den Betroffenen in Anspruch genommen werden können, erweist sich die Schweiz im internationalen Vergleich als gut ausgestattet; teilweise werden Betroffenen sogar rechtliche Möglichkeiten gegeben, die sich in anderen Ländern nicht finden lassen. Insgesamt erweist sich die Varianz zwischen den Ländern in diesem Bereich jedoch als nicht besonders gross.

Aufsichtsbehörde: EDÖB vergleichsweise schwach ausgestattet

Die Unabhängigkeit und die organisatorische Einbettung des EDÖB sind mit der Situation in anderen Ländern vergleichbar. Insbesondere nach der neusten Reform hat sich die Schweiz in dieser Hinsicht in den letzten Jahren der Mehrheit der untersuchten Länder angenähert.

Die grössten Unterschiede, welche sich im Rahmen des Rechtsvergleichs ergeben haben, beziehen sich auf die Kompetenzen der Aufsichtsstelle. Dabei zeigte sich, dass der EDÖB im internationalen Vergleich eher schwach ausgestattet ist. Andere Länder kennen im Bereich der Informationsbeschaffung im Rahmen der Aufsichtstätigkeit teilweise weitergehende Regelungen. Ein bedeutsamer Unterschied liegt in der Möglichkeit der meisten ausländischen Datenschutzbehörden, Vorabkontrollen durchzuführen. Diese Regelung, bestimmte Datenbearbeitungen im Voraus kontrollieren und genehmigen zu können, gibt der Aufsichtstätigkeit durch die Datenschutzbehörde einen präventiven Charakter. Die aktuellen Kompetenzen des EDÖB im Aufsichtsbereich sind hingegen primär darauf ausgerichtet, durch Sachverhaltsabklärungen und gegebenenfalls Empfehlungen bereits geschehene Missbräuche anzugehen, oder unmittelbar bevorstehende Verletzungen des DSG zu verhindern (Beantragung vorsorglicher Massnahmen).

Darüber hinaus sind auch die Sanktionsmöglichkeiten der schweizerischen Aufsichtsstelle vergleichsweise bescheiden: Der EDÖB kann weder direkt eine konkrete Datenbearbeitung verbieten, noch kann er eine direkte Busse an einen fehlbaren Datenbearbeiter aussprechen. Diese Möglichkeiten sind in den untersuchten Ländern zwar nicht flächendeckend, doch aber mehrheitlich gegeben. Der EDÖB seinerseits ist darauf angewiesen, seine Empfehlungen, falls sie vom Adressaten nicht umgesetzt werden, auf dem Gerichtsweg durchzusetzen, was sich als ressourcenintensiv erwiesen hat. Bezüglich der Ressourcenausstattung ist die schweizerische Aufsichtsstelle im Vergleich mit eher wenig Mitteln ausgestattet.

Technologiebezogene Regelungen

Das schweizerische Datenschutzgesetz ist technologieneutral ausgestaltet. Demgegenüber finden sich in den Datenschutzgesetzen anderer Länder spezifische, technologiebezogene Regelungen (bspw. zur Videoüberwachung, Biometrie). Auch in den untersuchten Gliedstaaten der USA (Massachusetts und Kalifornien) gibt es im Datenschutzbereich Regelungen zu bestimmten Anwendungen. Eine Einschätzung der Wirksamkeit solcher technologiebezogener Bestimmungen kann aufgrund der vorliegenden Informationen im Rechtsvergleich nicht vorgenommen werden. In Bezug auf die Situation in der Schweiz kann angeführt werden, dass die Technologieneutralität im DSG von den meisten Interviewpartnern – inklusive dem EDÖB – als sinnvoll eingestuft worden ist, da es für den Gesetzgeber schwierig sei, mit den rasanten Entwicklungen im Technologiebereich Schritt zu halten.

Fazit: Durchsetzungsrechte vergleichsweise gut, Aufsichtskompetenzen eher schwach ausgebaut

Die im DSG verankerten Durchsetzungsrechte erweisen sich vergleichsweise gut ausgebaut. Demgegenüber sind die Kompetenzen des EDÖB im internationalen Vergleich eher schwach. Anzumerken bleibt, dass die Wirksamkeit der soeben erwähnten zusätzlichen Kompetenzen (In-

formationsbeschaffung, Vorabkontrolle, Sanktionierung, Ressourcen) im Rahmen der Evaluation und des Rechtsvergleichs nicht empirisch untersucht wurde.

14.2.4 Referenzgrösse 4: verfassungsmässiger Mindestschutz

Art. 13 Abs. 2 BV statuiert – auch wenn dies aus der Formulierung der Bestimmung nicht klar hervorgeht – das Recht auf informationelle Selbstbestimmung. Dieses Recht umfasst den gesamten Umgang mit personenbezogenen Daten und kann nur unter den in Art. 36 BV genannten Voraussetzungen, d.h. gestützt auf eine gesetzliche Grundlage, nur bei Vorliegen öffentlicher Interessen oder zum Zweck des Schutzes von Grundrechten Dritter sowie unter Wahrung des Verhältnismässigkeitsgrundsatzes und des Kerngehalts der Grundrechte, eingeschränkt werden.

Insbesondere bei der Datenbearbeitung durch Bundesorgane fällt auf, dass sehr oft spezialgesetzliche Regelungen, in der Form eines Bundesgesetzes die Bearbeitung im konkreten Fall rechtfertigen[255]. Angesichts der fehlenden Möglichkeit des Bundesgerichtes, Bundesgesetze auf ihre Verfassungskonformität hin zu überprüfen, kann nicht gerichtlich garantiert werden, dass diese spezialgesetzlichen Grundlagen den verfassungsrechtlichen Anforderungen tatsächlich gerecht werden. Inwieweit und für welche Bereiche dies in der Praxis zu einer tatsächlichen Beschränkung des Grundrechts auf informationelle Selbstbestimmung geführt haben könnte, kann im Rahmen dieser Evaluation nicht überprüft werden, da es den Rahmen der Untersuchung sprengen würde.

Fazit: Keine Garantie für Mindestschutz

Aufgrund der fehlenden Verfassungsgerichtsbarkeit für Bundesgesetze besteht insbesondere bei Spezialgesetzen, welche eine Datenbearbeitung durch Bundesorgane ermöglichen, keine verwaltungsexterne Kontrolle, ob der grundrechtlich garantierte Mindestschutz der Betroffenen gewährleistet ist. Ob und in welchem Mass dies Grundrechte einschränken könnte, konnte im Rahmen dieser Evaluation nicht untersucht werden.

[255] Oben diskutiert wurden insbesondere die spezialgesetzlichen Bestimmungen im Bereich der Kranken- und Unfallversicherung (KVG und UVG).

15 Ausgewählte Handlungsoptionen

Nachdem im vorherigen Kapitel die wesentlichen Ergebnisse der Evaluation zusammengefasst worden sind und eine Bilanz über die Wirksamkeit des Datenschutzes gezogen worden ist, sollen in diesem Kapitel einige mögliche Handlungsoptionen im Hinblick auf die Erhöhung der Wirksamkeit des Datenschutzgesetzes kurz angedacht werden. Diese knüpfen entweder an die Ergebnisse der Untersuchung an oder sind vor dem Hintergrund laufender Reformbestrebungen auf europäischer Ebene zu sehen. Letztere sind im Bericht bisher nicht eigens thematisiert worden, sind aber Gegenstand der Ausführungen in Ziffer 15.3.

Da das Schwergewicht der Evaluationstätigkeiten auf der Erhebung der gegenwärtigen Situation lag, wird im Folgenden nicht der Anspruch erhoben, ein umfassendes, in sich ausgereiftes Konzept möglicher Verbesserungen bzw. Handlungsoptionen auf der gesetzgeberischen Ebene vorzustellen. Die einzelnen nachfolgend dargestellten Handlungsoptionen werden somit erstens nicht umfassend diskutiert und bewertet, sondern lediglich kurz hergeleitet und skizziert. Auch der Frage, inwieweit die Handlungsoptionen kombinierbar sind, und wo sich allenfalls Zielkonflikte ergeben, wird nur am Rand Beachtung geschenkt. Es ist zweitens festzuhalten, dass die Liste der aufgeführten Handlungsoptionen keinen Anspruch auf Vollständigkeit erheben kann; basierend auf den gemachten Befunden sind auch andere Massnahmen denkbar. Die Liste der hier thematisierten Handlungsoptionen ist drittens auch deshalb nicht als abschliessend zu betrachten, weil die vorliegende Evaluation nicht den Anspruch erhoben hat, sämtliche Aspekte des DSG umfassend abzubilden. Insbesondere wurde der Koordination zwischen Bund und Kantonen im föderalen Gesamtsystem der Schweiz und der internationalen Rechtsentwicklung, namentlich in der EU, und ihrer Auswirkungen auf die Schweiz, wenig Beachtung geschenkt (vgl. aber die Hinweise unter Ziffer 15.3.). So wird zum Beispiel die grundsätzliche Frage, wie die Zuständigkeiten von Bund und Kantonen bezüglich des Datenschutzes optimal aufzuteilen sind, hier nicht angesprochen.

Insofern kommt den nachfolgenden Ausführungen eher der Charakter von Gedankenanstössen als derjenige eines Arbeitspapiers im Hinblick auf die Formulierung im Einzelnen analysierter Vorschläge zu. Vielmehr müsste eine umfassende Diskussion über den Reformbedarf des DSG in einem weiteren Schritt geführt werden, wobei unter anderem an die nachfolgenden Überlegungen angeknüpft werden könnte.

Fast notwendigerweise handelt es sich aufgrund der festgestellten Grenzen des DSG um Handlungsoptionen, die darauf abzielen, den Datenschutz zu verstärken. Nachdrücklich sei jedoch darauf hingewiesen, dass es Sache des Gesetzgebers ist zu entscheiden, ob, wie stark und auf welchem Weg der Datenschutz gestärkt werden soll oder aber gewisse Einschränkungen der Persönlichkeitsrechte der Betroffenen zugunsten anderer Interessen und Werte vorgesehen werden sollen, wobei immer auch der völker- und verfassungsrechtliche Rahmen zu beachten ist.

Die weiterreichenden Handlungsoptionen, welche in der Regel auch eine Revision des DSG nach sich ziehen würden, werden im zweiten Teil des Kapitels vorgestellt. Aus der Evaluation haben sich daneben auch Anpassungspotenziale ergeben, die sich primär auf die praktische Anwendung des Gesetzes durch den EDÖB und die Bundesorgane beziehen. Diese werden gleich nachfol-

gend in Form von Empfehlungen im ersten Abschnitt des Kapitels behandelt. Sie knüpfen direkt an die Ausführungen in Teil IV der Evaluation an. Im dritten Teil erfolgen abschliessend einige Bemerkungen zur Einbettung des schweizerischen Datenschutzrechts in den internationalen bzw. europäischen Kontext.

15.1 Praktische Empfehlungen

Die nachfolgend aufgeführten Empfehlungen haben eher praktischen Charakter und sind insofern für die Wirksamkeit und Ausrichtung des Datenschutzgesetzes von geringerer Bedeutung als die unter Ziffer 15.2 diskutierten Handlungsoptionen. Sie beziehen sich auf den EDÖB und dessen Zusammenarbeit mit der Bundesverwaltung.

Dokumentation der Aktivitäten/Tätigkeitsbericht

Im Rahmen dieser Evaluation war es aufgrund der Datenlage teils nicht möglich, vollständige Angaben über die Aktivitäten des EDÖB sowie deren Auswirkungen zu erhalten. Nicht erhältlich waren insbesondere vollständige Angaben über die Anzahl durchgeführter Sachverhaltsabklärungen und die Quote von Sachverhaltsabklärungen, die mit einer Empfehlung endeten. Auch über die Stellungnahmen zu Vorlagen der Bundesbehörden mit einem Bezug zum Datenschutz existiert beim EDÖB keine Statistik. Weiter ist es auch nicht möglich aufzuschlüsseln, welchen Aufwand der EDÖB im Zusammenhang mit Datenbearbeitungen von Bundesorganen oder Privaten betreibt, und wie sich sein Beratungsaufwand gegenüber Betroffenen und Datenbearbeitern aufteilt. Solche Daten sind jedoch für die Steuerung der Aktivitäten nützlich und in der Kommunikation nach aussen – auch als Leistungsausweis des EDÖB – von Interesse.

Die hier angesprochenen Angaben könnten der Behörde als Grundlage für einen bilanzierenden Teil ihres Jahresberichts dienen. Aktuell zieht der EDÖB weder in seinem Tätigkeitsbericht noch an anderer Stelle systematisch und regelmässig Bilanz über seine Aktivitäten und Erfolge bzw. Misserfolge. Die heute im Tätigkeitsbericht ausgewiesenen Leistungsdaten sind zu wenig differenziert und erfüllen diese Anforderung nicht. Der EDÖB ist als weisungsunabhängige Behörde zwar dem Bundesrat und der Verwaltung nicht Rechenschaft schuldig, jedoch der Bundesversammlung und der Öffentlichkeit, die ihn finanziert. Das Fehlen einer zusammenfassenden und bilanzierenden Perspektive in den Jahresberichten zum Datenschutz allgemein und zu seinem Wirken im Besonderen erweckt nach aussen hin bis zu einem gewissen Grad das Bild einer Behörde, die ohne klares Konzept, inputorientiert und zufällig punktuell agiert, obwohl dies nicht zutrifft. Auch eine etwas systematischere Beschreibung und Analyse der wichtigsten Herausforderungen und Probleme des Datenschutzes aus der Sicht der höchsten Datenschutzbehörde des Bundes im Tätigkeitsbericht wäre wünschenswert, könnte sie doch als hilfreicher Orientierungspunkt für die öffentliche Diskussion dienen, und die jeweiligen Tätigkeitsschwerpunkte des EDÖB plausibilisieren.

4 *Empfehlung:* Der *EDÖB verbessert die Dokumentation seiner Aktivitäten dergestalt, dass seine elementaren Leistungsdaten laufend aktuell oder zumindest jährlich vollständig abrufbar sind. Diese Daten werden z.B. im Tätigkeitsbericht gegenüber der Öffentlichkeit ausgewiesen.*

4 *Empfehlung: Der EDÖB ergänzt seinen Tätigkeitsbericht um ein Kapitel, in dem er eine Bilanz seiner Aktivitäten und seines Erfolgs zieht, und in dem er die wichtigsten Entwicklungen und Herausforderungen im Bereich des Datenschutzes thematisiert und analysiert.*

Rollenteilung EDÖB-Bundesverwaltung

Die Verteilung der Aufgaben in Bezug auf den Datenschutz in den Bundesorganen, die durch Datenschutzberater der Bundesverwaltung einerseits und den EDÖB andererseits erbracht werden müssen, war schon mehrmals Gegenstand von Auseinandersetzungen zwischen dem EDÖB und der Bundesverwaltung (vgl. GPK-N 2003; EFK 2007). Sie wurde im Rahmen der vorliegenden Evaluation nicht umfassend untersucht. Gleichwohl zeigte sich im Rahmen der durchgeführten Gespräche, dass weder die Erwartungen des EDÖB an die Bundesorgane noch die Erwartungen der Bundesorgane an den EDÖB vollumfänglich erfüllt werden, und beidseits noch immer eine gewisse Unzufriedenheit besteht. Hier sind eine verbesserte Koordination und eine Klärung der Rollen angezeigt.

Die Verwaltung wünscht sich tendenziell eine Ausdehnung der Beratung seitens des EDÖB. Es erscheint jedoch klar, dass sich die Beratungstätigkeit des EDÖB schon angesichts seiner knappen Ressourcen auf einzelne, zentrale Projekte der Bundesverwaltung zu fokussieren hat. Es ist zu hoffen, dass die neu eingeführten Ausbildungsmöglichkeiten zur Klärung der Rollen beitragen. Zudem ist der Verordnungsvorschrift, wonach der Verkehr zwischen den Bundesorganen und dem EDÖB via die Datenschutzberater zu erfolgen hat, konsequent nachzuleben. Dies vereinfacht einerseits den Kommunikationsfluss zwischen der Verwaltung und dem EDÖB und stärkt andererseits die Datenschutzberater in den Bundesstellen.

4 *Empfehlung: In gemeinsamen Gesprächen klären der EDÖB und das zuständige Gremium der Bundesverwaltung (Interdepartementale Arbeitsgruppe Datenschutz, andere), wie eine künftige Aufgabenteilung aussehen sollte. Denkbar ist auch eine verstärkte Koordination der Beratungswünsche seitens der Departemente an den EDÖB, z.B. durch die interdepartementale Arbeitsgruppe Datenschutz.*

15.2 Weitere Handlungsoptionen

In den nachfolgenden Unterabschnitten werden einige Handlungsoptionen vorgestellt. Ihre allfällige Umsetzung erfordert in der Regel auch ein gesetzgeberisches Tätigwerden, und sie weisen einen grundsätzlicheren Charakter als die obigen, eher praxisorientierten Empfehlungen. Es werden somit nachfolgend nicht Empfehlungen ausgesprochen, sondern lediglich mögliche Handlungsoptionen zusammengestellt, die aufgrund der Ergebnisse der vorliegenden Untersuchung vertieft diskutiert werden könnten oder vor dem Hintergrund der laufenden Reformbestrebungen auf europäischer Ebene von Interesse sind (vgl. auch die einleitenden Bemerkungen zu diesem Kapitel sowie Ziffer 15.3). Wie bereits zu Beginn des Kapitels erwähnt, wird im Folgenden nicht der Anspruch erhoben, ein umfassendes, in sich ausgereiftes Konzept möglicher Verbesserungen, vorzulegen. Dies hätte den Rahmen der Evaluation gesprengt, lag doch deren Schwerpunkt auf der Erhebung der Ist-Situation.

Die nachfolgend aufgeführten Handlungsoptionen werden nach den verschiedenen Wirkungsmechanismen gegliedert, auf die sie sich beziehen, bzw. in Bezug auf welche sie potenziell Verbesserungen erbringen könnten. Zunächst werden Optionen erwähnt, die sich aus der Analyse des Prozesses der Durchsetzungsrechte ergeben haben. Es folgen Massnahmen, die sich auf die Ressourcen und die Aktivitäten des EDÖB beziehen. Im Weiteren geht es um Handlungsoptionen, welche auf eine stärkere präventive Wirkung des Gesetzes zielen, und um Optionen, mit denen versucht werden könnte, auf die neuen technologischen Herausforderungen zu reagieren. Abschliessend wird kurz auf die Frage zusätzlicher Sensibilisierungsaktivitäten eingegangen.

15.2.1 Zu den Einsichts- und Durchsetzungsrechten

Auskunft und Information

Das Auskunftsrecht nach Art. 8 DSG hat sich insgesamt wohl bewährt, so dass es sich nicht aufdrängt, die diesbezüglichen Rechtsgrundlagen zu modifizieren. Im Vergleich zur Vielzahl an Datenbearbeitungen, die vermutlich ohne Wissen der Betroffenen erfolgen, ist zwar die Zahl an Gerichtsfällen nicht sonderlich hoch. Immerhin hat sich eine Gerichtspraxis etabliert, welche die Einsichtsrechte gut schützt. Insbesondere erschiene es nicht oder allenfalls nur sehr schwer möglich, die Schranken des Auskunftsrechts – insbesondere soweit die ihm (möglicherweise) entgegenstehenden öffentlichen oder privaten Interessen betroffen sind – weiter zu präzisieren, da hier Interessenabwägungen eine entscheidende Rolle spielen, deren Durchführung bzw. Ergebnisse sich einer abstrakt-generellen Regelung letztlich entziehen.

Erwägenswert wäre jedoch eine Ausweitung der Informationspflicht für Private über Datenbeschaffungen und Datenbearbeitungen, da sich – auch aufgrund der relativ geringen Zahl an gerichtlichen Streitigkeiten in Bezug auf Auskunftsrechte gegenüber Privaten – der Eindruck aufdrängt, hier könnte die Wahrnehmung des Auskunftsrechts insofern auf Schwierigkeiten stossen, als die Betroffenen möglicherweise gar nicht über eine sie betreffende Datenbearbeitung informiert sind. Eine verstärkte Informationspflicht hätte somit den Zweck, über erfolgte oder beabsichtigte Datenbearbeitungen Transparenz zu schaffen und vom heutigen grundsätzlichen Prinzip der Holschuld des Betroffenen tendenziell zu einer Bringschuld des Bearbeiters überzugehen. Dieser Ansatz erhöhte letztlich die Transparenz von Datenbearbeitungen und stünde im Übrigen auch im Einklang mit den Anforderungen der RL 95/46 (vgl. Art. 10, 11 RL 95/46), wobei die Transparenzpflichten der RL 95/46 im Zuge der Revision des EU-Datenschutzrechts noch ausgeweitet werden sollen. Er ist auch Teil der derzeit laufenden Überlegungen im Hinblick auf die Erarbeitung eines weiteren Zusatzprotokolls zur Datenschutzkonvention des Europarates (vgl. Ziffer 15.3). Denkbar ist dabei auch, dass Betroffene durch explizite Erklärung auf die Information verzichten können. Deutschland kennt eine entsprechende Regelung (SIR 2010: 75).

Durchsetzungsrechte gegenüber privaten Datenbearbeitern

Art. 15 DSG gibt den Betroffenen das Recht auf Löschung, Sperrung, Berichtigung und Vermerkung bei Datenbearbeitungen von Privaten. Wie die Evaluation gezeigt hat, dürfte dieser Bestimmung kaum eine eigenständige Bedeutung zukommen; letztlich erlangt sie nur zusammen mit

Art. 28 ZGB eine gewisse Bedeutung. Aber auch darüber hinaus spielt Art. 15 DSG in der gerichtlichen Praxis insgesamt eine untergeordnete Rolle. Denn häufig scheuen sich Private, im Falle einer Persönlichkeitsverletzung den Rechtsweg – entsprechend der Grundkonzeption des Art. 15 DSG – zu bestreiten, wohl in erster Linie weil das Prozess- und Kostenrisiko als unverhältnismässig angesehen wird. Diese Überlegung kommt wohl insbesondere immer dann zum Tragen, wenn eine widerrechtliche Persönlichkeitsverletzung als nicht „gravierend" angesehen wird und (bisher) zu keinen materiellen Schäden geführt hat. Diese Hypothese wird durch die relative Seltenheit der Beschreitung des Rechtsweges gestützt.

Aufgeworfen wird damit die Frage, ob es nicht sinnvoll sein könnte, über eine Verstärkung der Möglichkeiten der Privaten, ihre Rechte durchzusetzen bzw. über alternative Durchsetzungsmechanismen nachzudenken: Denn die erwähnten Defizite implizieren, dass – sozusagen systemimmanent – eine Reihe widerrechtlicher Persönlichkeitsverletzungen gerade nicht festgestellt und gegebenenfalls auch nicht eingestellt wird. Jedoch ist zu beachten, dass auch vermeintlich „harmlose" Persönlichkeitsverletzungen mitunter für die Betroffenen nicht vorhersehbare Konsequenzen entfalten können, ganz abgesehen davon, dass das DSG grundsätzlich davon ausgeht, dass jede widerrechtliche Persönlichkeitsverletzung zu unterbleiben hat. Zu diskutieren wären deshalb effektive Mechanismen im Hinblick auf die (gerichtliche) Geltendmachung und Feststellung solcher Persönlichkeitsverletzungen.

In Betracht könnten hier etwa folgende Mechanismen kommen:

- Soweit es um alternative Lösungsansätze geht, könnte man hier insbesondere an die Einführung einer Art Verbandsklage denken, deren genaue Voraussetzungen aber selbstverständlich noch zu präzisieren wären. Die Idee hinter der Verbandsklage ist, die Individuen vom Prozessrisiko zu entlasten und dieses einer potenten und juristisch kompetenten Fachorganisation zu überlassen. Auch im Rahmen der bevorstehenden Revision der Datenschutzkonvention des Europarates (vgl. Ziffer 15.3) wird über eine Erweiterung des zu gewährenden Rechtsschutzes, insbesondere im Hinblick auf eine Rekursmöglichkeit juristischer Personen, nachgedacht. Im Zuge der Revision des EU-Datenschutzrechts (vgl. Ziffer 15.3) will die Kommission prüfen, ob die Befugnis zur Klage bei nationalen Gerichten auch auf Verbände der Zivilgesellschaft sowie andere Verbände, die die Interessen der von der Datenbearbeitung Betroffenen vertreten, ausgedehnt werden soll.

- Darüber hinaus und davon unabhängig könnten auch Erleichterungen des gerichtlichen Zugangs, insbesondere soweit die Kosten betroffen sind, in Erwägung gezogen werden. Im Einzelnen wäre hier aber zu eruieren, wie sich eine solche Massnahme in die geltenden zivilprozessrechtlichen Strukturen einbetten liesse.

- Ergänzend hierzu könnte auch die explizite Zurverfügungstellung spezifisch auf datenschutzrechtliche Streitigkeiten ausgerichteter aussergerichtlicher Streitbeilegungsmechanismen (insbesondere Mediation) in Betracht gezogen werden.

- Das DSG kennt keinen spezifischen Schadensersatzanspruch im Fall der Verletzung der datenschutzrechtlichen Vorgaben, dies im Gegensatz zu ausländischen Rechtsordnungen (vgl. etwa für Deutschland § 7 BDSG) und zu Art. 23 Abs. 1 RL 95/46. Es könnte daher

überlegenswert sein, eine spezifisch datenschutzrechtliche Schadensersatzpflicht einzuführen, womit der effektiven Beachtung der datenschutzrechtlichen Vorgaben Vorschub geleistet werden könnte, entfaltete doch ein solches Instrument wohl auch eine präventive Wirkung. Ein solcher spezifischer Schadensersatzanspruch könnte es ermöglichen, den Spezifika der Verletzung datenschutzrechtlicher Vorgaben Rechnung zu tragen. Im Einzelnen wäre die Ausgestaltung eines solchen Anspruchs auch im Vergleich zu den bestehenden Vorgaben des OR zu präzisieren, wobei die Rechtslage in anderen Staaten (die, wie erwähnt, einen solchen spezifischen Anspruch neben den allgemeinen zivilrechtlichen Ansprüchen kennen) zu berücksichtigen wäre.

- Weiter könnte über eine allgemeine Anzeigepflicht für Datenschutzverstösse nachgedacht werden (wobei insbesondere die Adressaten derartiger Anzeigen sowie die eine Anzeigepflicht begründenden Umstände zu präzisieren wären). Dieses Instrument wird im Zuge der Revision des EU-Datenschutzrechts (vgl. Ziffer 15.3) erwogen.
- Schliesslich ist zu fragen, ob ein grundsätzliches Widerspruchsrecht der Betroffenen in Bezug auf eine Datenbearbeitung – was insbesondere dann relevant ist, wenn die Datenbearbeitung nicht auf einer Einwilligung beruht, so dass es ein Widerspruchsrecht ermöglichte, dass die Betroffenen sich in jedem Fall einer Datenbearbeitung widersetzen könnten – die Position der Betroffenen gegenüber den privaten Datenbearbeitern stärken könnte. Ein solches Recht, dessen genaue Konturen noch der Präzisierung bedürften, ist durch die RL 95/46 aufgegeben und findet sich demnach auch in der Rechtsordnung zahlreicher europäischer Staaten (vgl. z.B. für Deutschland §§ 20 Abs. 2, 28 Abs. 4, 29 Abs. 4, 35 Abs. 5 BDSG). Derzeit diskutiert wird es auch im Rahmen der Reformbestrebungen der Datenschutzkonvention des Europarates, und im Zuge der Revision des EU-Datenschutzrechts wird erwogen, die Tragweite dieses Grundsatzes durch verschiedene Instrumente (insbesondere ein „Recht auf Vergessen“ und ein Recht des Einzelnen, seine einmal zur Verfügung gestellten Daten „zurückholen“ zu können) zu erweitern (vgl. Ziffer 15.3.).

Zur Durchsetzung gegenüber Bundesorganen und zur Rolle spezialgesetzlicher Regelungen

Art. 25 DSG garantiert Durchsetzungsrechte gegenüber Bundesorganen. Er ist Gegenstand einiger Urteile der höheren Gerichte. Allerdings beziehen sich die meisten Begehren auf die Berichtigung (vermeintlich) unrichtiger Daten. Soweit es vor Gericht um die Zulässigkeit einer Datenbearbeitung als solche geht, steht in der Regel die Existenz einer (ausreichenden) gesetzlichen Grundlage zur Debatte.

Aufgrund dieser Massgeblichkeit der spezialgesetzlichen Grundlagen sind diese in der Regel entscheidend für die Zulässigkeit der Datenbearbeitung; angesichts der fehlenden Verfassungsgerichtsbarkeit in der Schweiz kann in diesem Rahmen jedoch nicht geprüft werden, ob diese spezialgesetzlichen Grundlagen immer auch den verfassungsrechtlichen Anforderungen gerecht werden. Zu erinnern ist in diesem Zusammenhang aber an die verwaltungsinterne Rechtsetzungsbegleitung, in deren Rahmen diese Aspekte analysiert werden, dies im Hinblick sowohl auf die Beachtung der verfassungs- und völkerrechtlichen Vorgaben als auch die Sicherstellung einer gewissen Kohärenz in der Gesetzgebung.

Die allgemeinen Grundsätze der Datenbearbeitung (Art. 4 DSG) sind nach der Rechtsprechung des EGMR Ausfluss der grundrechtlichen Garantie des Art. 8 EMRK[256], so dass sie – zumindest soweit es um das Verhalten von Bundesorganen geht – nicht zur Disposition des Gesetzgebers stehen. In der Rechtsprechung ist jedoch das Verhältnis der Spezialgesetzgebung zu den allgemeinen Grundsätzen des DSG nicht immer ganz klar formuliert, wird doch mitunter betont, das DSG finde im Falle der Einschlägigkeit einer spezialgesetzlichen Grundlage keine Anwendung mehr, wobei teilweise unklar bleibt, ob dies auch bedeutet, dass die allgemeinen Bearbeitungsgrundsätze nicht zu beachten wären[257]. Daher fragt es sich, ob die erwähnte grundsätzliche allgemeine Massgeblichkeit der datenschutzrechtlichen Grundsätze ausdrücklich verankert werden soll; so ist es interessant, dass Art. 8 Abs. 2 Grundrechtecharta die zentralen datenschutzrechtlichen Grundsätze auf primärrechtlicher Stufe festhält. Dem würde in der Schweiz eine sinngemässe Ergänzung des Art. 13 Abs. 2 BV entsprechen; grundsätzlich in Betracht käme aber auch eine klarstellende Ergänzung des DSG, etwa indem in den 4. Abschnitt des DSG („Bearbeiten von Personendaten durch Bundesorgane“) eine Bestimmung eingefügt wird, wonach im Falle der Bearbeitung von Personendaten durch Bundesorgane die in Art. 4 DSG formulierten Anforderungen kumulativ neben ggf. einschlägigen spezialgesetzlichen Regelungen zu beachten sind.

Darüber hinaus wäre zu überlegen, ob die Verbindung zwischen dem Datenschutzgesetz als allgemeiner Rahmen und Konkretisierung verfassungsrechtlicher Vorgaben für die Zulässigkeit von Datenbearbeitungen einerseits und den jedenfalls notwendigen Spezialgesetzen andererseits nicht auch prozedural verstärkt werden könnte, etwa indem bei der Formulierung gesetzlicher Grundlagen für Datenbearbeitungen einheitliche „Standards“ vorgesehen werden, deren Einhaltung durch eine Art formalisierte „Datenschutzverträglichkeitsprüfung“ – deren Grundgedanken sich an die Umweltverträglichkeitsprüfung anlehnen könnten – sichergestellt wird. Auf diese Weise könnte auch sichergestellt werden, dass die spezialgesetzlichen Grundlagen für die Datenbearbeitung „einheitlicher“ ausgestaltet sind, was ihre Auslegung und Anwendbarkeit erleichterte. Dabei müsste die genaue Ausgestaltung und Funktionsweise dieses Instruments noch im Einzelnen präzisiert werden.

Schliesslich ist im Zusammenhang mit der Durchsetzung gegenüber Bundesorganen noch zu erwähnen, dass die oben angesprochenen Instrumente der Verbandsklage, des Widerspruchsrechts, eines Schadenersatzanspruchs sowie einer allgemeinen Anzeigepflicht für Datenschutzverstösse auch im Zusammenhang mit der Datenbearbeitung durch Bundesorgane in Erwägung gezogen werden könnten.

---

256 Vgl. etwa EGMR, Nr. 7508/02, Urt. v. 10.10.2006, L.L./Frankreich (Grundsatz von Treu und Glauben); EGMR, Urt. v. 27.8.1997, Rec. 1997-IV, M.S./Schweden (Grundsatz der Zweckbindung); EGMR, Nr. 62332/00, Urt. v. 6.6.2006, Peck/Grossbritannien (Grundsatz der Verhältnismässigkeit); EGMR, Nr. 63737/00, Urt. v. 17.7.2003, Perry/Grossbritannien (Freiwilligkeit der Einwilligung nach erfolgter genügender Information).

257 Z.B. BGE 133 V 359, 363.

15.2.2 Ressourcen des EDÖB und Hinweise zur Gewichtung seiner Aktivitäten

Wie oben festgestellt wurde, sind die Ressourcen des EDÖB im Vergleich zu seinen Aufgaben nach allgemeiner Einschätzung zu knapp bemessen. Hievon ausgehend kann vermutet werden, dass sich eine Wirkungssteigerung durch einen allgemeinen Ausbau der Mittel der Datenschutzbehörde – unabhängig von den nachfolgend aufgeführten und teils mit Kosten verbundenen Optionen – erzielen liesse.

Verbunden mit einem Mittelausbau stellt sich die Frage nach dem optimalen Einsatz zusätzlicher Mittel, wobei der Aspekt der richtigen Gewichtung der verschiedenen gesetzlichen Aufgaben des EDÖB von genereller Natur ist. Auch diese Diskussion kann hier nicht abschliessend geführt werden. Einige Hinweise sind jedoch möglich: Grundsätzlich ist festzuhalten, dass der EDÖB in der Aufteilung seiner Mittel und der Gewichtung der ihm gesetzlich übertragenen Aufgaben frei ist, was als Ausdruck seiner Unabhängigkeit verstanden werden kann (Huber 2006: 370). Wenig überraschend sind weiter die Befunde dieser Evaluation, wonach die Bearbeiter sich primär einen beratenden EDÖB wünschen, wobei insbesondere in der Bundesverwaltung tendenziell ein Ausbau der Beratungstätigkeit gewünscht wird (vgl. Empfehlung unter Ziffer 15.1); die Betroffenen hingegen befürworten durchaus auch eine Behörde, die „zum Rechten schaut". Bei einer allfälligen Umgewichtung der Mittel ist neben den divergierenden Wünschen von Bearbeitern und Betroffenen schliesslich zu beachten, dass zwischen den verschiedenen Aufgabenbereichen des EDÖB Wechselwirkungen bestehen: Einerseits gibt es zwischen den Aktivitäten Synergien (Information als Rückgrat der Aufsicht und Beratung, Beratung als Informationsquelle des EDÖB), andererseits aber auch Störeffekte; in dieser Evaluation wurde insbesondere auf die Problematik hingewiesen, dass die Doppelrolle des EDÖB als Aufsichts- und Beratungsorgan dazu führt, dass bestimmte Bearbeiter den EDÖB meiden. Diese Aspekte sind bei einer Umgewichtung zu berücksichtigen (vgl. auch nachfolgende Handlungsoptionen).

15.2.3 Zur Aufsichtsfunktion des EDÖB

Die Evaluation hat dem EDÖB bezüglich seiner Aufsichtstätigkeit eine hohe Wirksamkeit im Einzelfall attestiert. Bei Widerstand des Datenbearbeiters sind jedoch seine Mittel sowohl bei der Beschaffung der Informationen als auch bei der Durchsetzung des DSG begrenzt (Art. 27 und Art. 29 DSG). Wie der Rechtsvergleich gezeigt hat, sind diesbezüglich die Aufsichtsbehörden anderer Länder teilweise mit stärkeren Mitteln ausgestattet. Bei der Feststellung des Sachverhalts kann er Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Dass der EDÖB somit stark auf die Kooperationsbereitschaft der Datenbearbeiter angewiesen ist, kann sich hinsichtlich der Effizienz, aber auch hinsichtlich der Effektivität seiner Sachverhaltsabklärungen potenziell als nachteilig erweisen. Zumindest bleibt für den EDÖB häufig eine Ungewissheit zurück, ob ihm im Rahmen der Abklärung die relevanten Informationen zugänglich gemacht wurden. Entsprechend könnte geprüft werden, ob die Befugnisse des EDÖB bei der Informationsbeschaffung ausgedehnt werden sollen. Denkbar ist prinzipiell, dem EDÖB das Recht einzuräumen, Akten zu konfiszieren und Datenbearbeitungen am Computer selbst anzuwenden. Andere Länder sehen ferner die Möglichkeit von direkten Bussen vor,

wenn der Bearbeiter der Aufsichtsbehörde Informationen vorenthält (Frankreich, Niederlande, Italien).

Wenn der EDÖB eine Anpassung oder die Einstellung einer Datenbearbeitung durchsetzen will, kann er diese zunächst nur empfehlen und muss bei Widerstand den Gerichtsweg einschlagen. Auch wenn der EDÖB im Einzelfall recht erfolgreich operiert, so sind Gerichtsverfahren mit einem beträchtlichen Aufwand verbunden. Zudem werden fehlbare Datenbearbeiter nicht gebüsst und das DSG sieht keinen spezifischen Schadenersatzanspruch für Geschädigte vor (vgl. zum zuletzt genannten Punkt schon Ziffer 15.2.1). Eine Ausdehnung der Sanktionsmöglichkeiten könnte die Einflussmöglichkeiten des EDÖB stärken. Eine Stärkung seiner Sanktionskompetenz könnte prinzipiell dadurch erfolgen, dass der EDÖB Massnahmen nicht empfehlen, sondern in Form einer anfechtbaren Verfügung erlassen könnte; die Last, im Konfliktfall den Fall vor Gericht zu ziehen, läge somit beim Bearbeiter und nicht mehr beim EDÖB. Eine zusätzliche Verschärfung der Sanktionskompetenz könnte über eine Bussenkompetenz erreicht werden, die mehrere Länder mit allerdings sehr unterschiedlichen Maximalbussen kennen. Wie ebenfalls im Rahmen des Rechtsvergleichs gezeigt wurde, verfügen die Aufsichtsbehörden in mehreren Ländern zudem über die Möglichkeit, Datenbearbeitungen zu verbieten; auch die Anordnung der Sperrung, Löschung oder Vernichtung ist in einer Mehrzahl der untersuchten Staaten möglich.

Eine weitere potenzielle Wirkungsgrenze, welche die Evaluation aufgezeigt hat, ist die Tatsache, dass der EDÖB nach Sachverhaltsabklärungen insbesondere im Privatbereich derzeit praktisch nie prüft, ob andere Bearbeiter mit ähnlichen Bearbeitungen die Bestimmungen einhalten. Diesbezüglich würde die Möglichkeit bestehen, dass der EDÖB durch stichprobenweise Zusatzkontrollen bei solchen Bearbeitern die Breitenwirkung seiner Empfehlungen besser absichern könnte als heute, wo er primär auf dem Weg der Veröffentlichung Druck zu erzeugen versucht. Obwohl in der Lehre tendenziell die Auffassung vertreten wird, der EDÖB lege seine Aufsichtskompetenz nach Art. 29 DSG bereits recht weit aus, überwiegt die Haltung, dass das DSG einer solchen Vorgehensweise nicht entgegenstehe. Eine Gesetzesrevision wäre somit für ein solches Vorgehen vermutlich nicht notwendig. Dem EDÖB zufolge sind solche Zusatzkontrollen mit den heutigen Ressourcen jedoch nicht möglich.

Eine Stärkung der Aufsichtsfunktion des EDÖB, wie sie mit den erwähnten Massnahmen beschrieben worden ist, geht tendenziell mit einem Wandel seiner Rolle einher. Bereits in der aktuellen Situation zeigten sich gewisse negative Folgen der Doppelfunktion des EDÖB als Beratungs- und Aufsichtsbehörde, wird er bei heiklen Anwendungen doch als Berater teilweise gemieden. Es ist zu vermuten, dass seine Bedeutung als Beratungsorgan weiter gemindert wird, wenn er verstärkt als Aufsichtsorgan wahrgenommen wird. Insofern drängt sich die Frage auf, ob dies durch eine verstärkte organisatorische Trennung der Beratungs- und der Aufsichtsfunktion kompensiert werden sollte.

Allen hier aufgeführten Massnahmen ist gemein, dass sie nur dann greifen, wenn der Datenbearbeiter dem EDÖB bekannt ist und wenn rechtlich eine Möglichkeit besteht, auf die Datenbearbeiter zuzugreifen. Insofern stossen sie bei den neuen Herausforderungen (Intransparenz, Bearbeitungen vom Ausland her) an Grenzen.

15.2.4 Präventiver Datenschutz: Organisatorische Massnahmen und Vorabkontrolle

Die bisher aufgeführten Handlungsoptionen zielen primär darauf ab, die Betroffenen und den EDÖB in Situationen zu stärken, in denen eine Datenbearbeitung bereits erfolgt und ein Schaden womöglich bereits eingetreten ist. Sowohl seitens der Betroffenen als auch der Bearbeiter ist es jedoch wünschenswert, mögliche Fehler bei Datenbearbeitungen von vornherein zu vermeiden. Bei der Bewertung der Beratungstätigkeit des EDÖB erwies sich denn auch als Mangel, dass die Ratschläge des EDÖB nicht verbindlich sind. Damit kann der EDÖB bei datenschutzsensitiven Projekten das Investitionsrisiko der Bearbeiter nicht oder nur unbefriedigend senken, weil er keine Garantieerklärung abgeben kann, dass eine Bearbeitung mit dem DSG in Einklang steht.

Bereits an anderer Stelle wurde auf die Problematik der Durchsetzung der Datenschutzgrundsätze verwiesen. Sie stösst in der Praxis insofern auf grosse Schwierigkeiten, als sie in beachtlichem Ausmass Beurteilungsspielräume einräumt bzw. Abwägungen impliziert. Diese können nicht nur je nach „politischem Zeitgeist" variieren und sind damit nicht nur mitunter schwer vorhersehbar, sondern stossen gerade im Datenschutzrecht auf die Schwierigkeit, dass letztlich ein „Wert" – nämlich das Recht auf Privatsphäre – in der Regel einem bestimmten „Nutzen" gegenübersteht, so dass es bei der Abwägung um verschiedene Kategorien von Rechtsgütern geht. Diese Problematik ist sowohl auf der Ebene der Gesetzgebung – sind doch häufig Spezialgesetze für die Zulässigkeit einer bestimmten Datenbearbeitung entscheidend (vergleiche oben) – als auch auf derjenigen der Gesetzesanwendung relevant. Daher könnte es sich aufdrängen, durch die Einführung zusätzlicher präventiv wirkender Verfahren die Effektivität der datenschutzrechtlichen Grundsätze zu verstärken.

Es stellt sich somit die Frage, welche Massnahmen bereits vor Inbetriebnahme von Datenbearbeitungen dazu beitragen können, dass diese DSG-konform ausfallen. Aus Sicht der Datenbearbeiter bedingen solche Massnahmen eine systematische und gründliche Auseinandersetzung mit den Fragen des Datenschutzes bereits in der Projektphase, was mit Mehraufwand bei der Planung und möglicherweise auch bei der Anwendung verbunden sein dürfte. Es ist auch nicht auszuschliessen, dass gewisse Datenbearbeitungen für die Nutzerinnen und Nutzer umständlicher werden, weil sie zum Beispiel verstärkt zu expliziten Einwilligungen aufgefordert werden müssen. Umgekehrt können die Bearbeiter ihr Investitionsrisiko senken, weil die Rechtmässigkeit ihrer Projekte verbindlich geprüft worden ist. Für die Betroffenen ihrerseits sinkt das Risiko einer unrechtmässigen Bearbeitung.

Einen Schritt in Richtung vorbeugender Massnahmen hat der Gesetzgeber bei seiner 2008 in Kraft getretenen Teilrevision des DSG getan, indem er die Verleihung von Datenschutzzertifikaten an private und öffentliche Datenbearbeiter ermöglicht hat (Art. 11 DSG). Es ist noch zu früh für eine Aussage, ob die Zertifizierung die erwünschte Wirkung erbringt. Gleichwohl sind weitere prozessuale Massnahmen denkbar, die in die Richtung eines verstärkt auf Prävention ausgerichteten Datenschutzes zielen. So könnte z.B. versucht werden, die Zertifizierung von Datenbearbeitungen (Art. 11 DSG) stärker zu fördern. Eine Option bestünde darin, die staatlichen Behörden einzubinden: Sie können verstärkt dazu angehalten werden, ihre eigenen Prozesse zertifizieren zu lassen. Darüberhinaus könnten die Bundesbehörden angehalten werden, ihre Nachfragemacht zugunsten zertifizierter Bearbeiter einzusetzen. Hier wäre näher zu prüfen, inwieweit

dies eine Anpassung des Beschaffungsrechts erfordern würde und inwieweit dies im Rahmen der bestehenden WTO-Normen überhaupt möglich wäre. Inwieweit die öffentlichen Stellen diesen Ansätzen bereits heute nachleben, kann hier nicht beurteilt werden. Analog könnten im Übrigen auch Bearbeiter bevorzugt werden, die über unabhängige Datenschutzverantwortliche nach Art. 11a Abs. 5 Buchstabe e DSG verfügen. Es ist allenfalls auch denkbar, solche für bestimmte Gruppen von Datenbearbeitern verbindlich vorzuschreiben. Jenseits der staatlichen Einflusssphäre hängt die Popularität der Zertifizierung und der Einführung unabhängiger Datenschutzverantwortlicher stark von der Datenschutzsensibilität der Betroffenen ab.

Während die Zertifizierung und die Einführung unabhängiger Datenschutzverantwortlicher auf Freiwilligkeit setzen (sieht man einmal von der erwähnten Möglichkeit ab, unter gewissen Voraussetzungen unabhängige Datenschutzverantwortliche für obligatorisch zu erklären, vgl. oben), ginge es sehr viel weiter, eine obligatorische Vorabkontrolle geplanter Datenbearbeitungen einzuführen. Bei einer solchen würde in Bezug auf ggf. näher zu präzisierende Datenbearbeitungen, die besondere Risiken für die Persönlichkeitsrechte der Betroffenen implizieren, eine Prüfung der Zulässigkeit der Datenbearbeitung und damit der Erfüllung der Rechtmässigkeitsanforderungen vor der Durchführung der Bearbeitung im Sinne einer Genehmigung eingeführt, so wie dies auf europäischer Ebene in Art. 20 der RL 95/46 angelegt ist und in sämtlichen untersuchten EU-Staaten umgesetzt wurde. Zwar wird auch hier das Investitionsrisiko der Datenbearbeiter gesenkt, primär zielt der Vorschlag aber auf einen verstärkten Schutz der Betroffenen. Hier wäre gegebenenfalls sorgfältig zu überlegen, unter welchen genauen Voraussetzungen eine solche Vorabkontrolle durchzuführen wäre und wie eine solche Kompetenz ins Pflichtenheft des EDÖB einzufügen wäre. Auch hier stellt sich zumindest die Frage nach einer organisatorischen Trennung dieses Kontrollbereichs von der Beratung (vgl. oben Vorschläge zur Aufsicht).

15.2.5 Vorschläge in Bezug auf die Herausforderungen durch neue Technologien

Im DSG gibt es keine Vorschriften, die sich spezifisch auf einzelne Technologien beziehen. Dieser Grundsatz der Technologieneutralität wird aufgrund des schnellen technologischen Wandels und der begrenzten Anpassungsfähigkeit von Gesetzesvorschriften auch von den interviewten Experten im Rahmen dieser Evaluation befürwortet, und auch im europäischen Umfeld sind technologiespezifische Regelungen in Datenschutzgesetzen nicht üblich.

Dies ändert aber nichts an der bestehenden Herausforderung des DSG und seiner Grundsätze durch neue Technologien. Die Evaluation hat gezeigt, dass die bisherigen Mechanismen der Durchsetzungsrechte und der Aufsicht gerade bei Bearbeitungen, die auf neuen Technologien beruhen, ins Leere laufen können. Auch die bisher diskutierten Massnahmen fussen primär auf der Annahme, dass Datenbearbeiter und Datenbearbeitungen transparent sind und somit allfällige Missachtungen des DSG bemerkt werden. Deshalb werden hier zwei Grundsätze aufgeführt, die insbesondere auf Datenbearbeitungen mit neuen Technologien zugeschnitten sind. Hierzu zählt erstens Stärkung des Grundsatzes „Privacy by Design“ und zweitens die Einführung des „Opt-in-Prinzips“[258].

[258] Auch „Privacy by Default“.

Das Prinzip des Privacy by Design verfolgt die Strategie, allfällige Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen sowie den Datenschutz von vornherein in die Gesamtkonzeption einzubeziehen, anstatt bestehende Datenschutzprobleme nachträglich durch Korrekturprogramme zu beheben (Schaar 2010)[259]. Schon heute verpflichtet Art. 7 DSG die Bearbeiter zur Gewährleistung der Datensicherheit mittels technischer und organisatorischer Massnahmen, was aber primär auf den Schutz vor unbefugten Zugriffen auf die Daten zielt (Pauli 2006: 114-125) und somit höchstens einen Teilaspekt von Privacy by Design abdeckt. Privacy by Design beinhaltet auch den Gedanken, dass Systeme so konzipiert und konstruiert sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente sind beispielsweise „die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung oder möglichst baldige Löschung personenbezogener Daten" (Schaar 2010: 267).

Zweitens ist an die Förderung des Opt-in-Prinzips als Präzisierung des Einwilligungsgrundsatzes – der auch im Rahmen der bevorstehenden Revision des EU-Datenschutzrechts überdacht bzw. präzisiert werden soll (vgl. Ziffer 15.3) – zu denken. Dieses Prinzip verlangt, dass z.B. Internetanwendungen bezüglich der vom Benutzer zur Verfügung gestellten Daten auf eine minimale Verwendung voreingestellt sind und jede Ausweitung der Bearbeitung vom Nutzer explizit bewilligt werden muss. Heute ist dies oft noch umgekehrt (Fraunhofer Institut 2008).

Auch wenn die in Art. 4 Abs. 5 DSG geregelten Grundsätze der Gültigkeit einer Einwilligung im Ansatz klar und einleuchtend sind (und auch durch die Rechtsprechung die genauen Anforderungen an eine gültige Einwilligung präzisiert und teilweise eher streng ausgelegt werden), ist doch nicht zu verkennen, dass ihre Anwendung auf zahlreiche praktische Fallgestaltungen je länger je mehr auf Schwierigkeiten stösst, so dass sich mitunter der Eindruck aufdrängt, zumindest gewisse Einwilligungen bzw. die Bejahung ihres Vorliegens beruhten letztlich auf einer Fiktion. Diese Entwicklung wird durch die zunehmende Bedeutung elektronischer Medien und insbesondere des Internet verstärkt. Eine angemessene Information der Betroffenen dürfte etwa auch dann zu verneinen sein, wenn in umfangreichen Allgemeinen Geschäftsbedingungen letztlich ungewöhnliche Datennutzungen vorgesehen sind (ohne dass auf diese ausdrücklich hingewiesen wird) oder wenn auf dem Internet ein unverhältnismässiger Aufwand betrieben werden muss, um gewisse Datennutzungen einzuschränken.

Es ist zu diskutieren, wie dem Opt-in-Prinzip und Privacy by Design insgesamt mehr Nachachtung verschafft werden könnte. Es fragt sich, ob es sich nicht aufdrängen könnte, durch eine entsprechende Klarstellung auf Gesetzes- oder Verordnungsebene entsprechende Anforderungen festzulegen. So liesse sich z.B. bezüglich des Opt-in-Prinzips verlangen, dass zumindest gewisse Einwilligungen (insbesondere im Rahmen der Internetnutzung) durch aktives Tätigwerden erfolgen müssen, so dass es nicht genügt, dass man etwa durch Ankreuzen gegen bestimmte Datenbearbeitungen opponiert, sondern – im Gegenteil – durch Ankreuzen diese Datenbearbeitungen erlauben muss. Dies implizierte letztlich, dass Einwilligungen in Datenbearbeitungen grundsätzlich ausdrücklich erfolgen müssen, wie dies für besonders schützenswerte Personendaten oder

[259] Vgl. im Einzelnen zum Konzept des „Privacy by Design" Mitteilung der Kommission „Eine digitale Agenda für Europa", KOM (2010) 245 endg.

Persönlichkeitsprofile vorgesehen ist und auch in Art. 7 Bst. a i.V.m. Art. 2 Bst. h RL 95/46 verankert ist.

Über die blosse Verankerung dieser Vorschriften hinaus stellt sich aber auch die Frage der tatsächlichen Umsetzung. Da insbesondere Privacy by Design die Berücksichtigung des Datenschutzes bereits in der Konzeptionsphase von Projekten vorsieht, scheint es sinnvoll, diesen Vorschlag mit den weiter oben beschriebenen präventiven Massnahmen zu koppeln. Im Rahmen von datenschutzrelevanten Bundesprojekten kann erwähnt werden, dass bei Informatikprojekten, die konsequent nach HERMES abgewickelt werden, der Datenschutz laut dem Befund der Finanzkontrolle durch organisatorische Massnahmen bereits „gebührend berücksichtigt" werde (EFK 2007: 17).

Schliesslich stellen sich nicht nur, aber insbesondere auch in Zusammenhang mit der technologischen Entwicklung Fragen zur Definition der Begriffe „Personendaten" und „besonders schützenswerte Personendaten". Der Anwendungsbereich des DSG knüpft an die Identifizierbarkeit einer Person an. Zwar wurde durch die Rechtsprechung der Begriff der identifizierbaren Person teilweise präzisiert, so wenn angenommen wird, auch Angaben über Objekte, die einer Person zugeordnet werden können, könnten Personendaten darstellen. Gleichwohl fragt es sich, ob und inwieweit (insbesondere angesichts der technischen Entwicklungen) nicht auch Angaben, die sich nicht auf eine identifizierbare Person zurückführen lassen, gewissen datenschutzrechtlichen Mindestanforderungen genügen müssten, insbesondere dann, wenn sich die spätere Möglichkeit der Rückführung auf eine identifizierbare Person nicht ausschliessen lässt. Dieser Themenkomplex wird derzeit auch im Rahmen der bevorstehenden Revision der Datenschutzkonvention des Europarates diskutiert wird (vgl. Ziffer 15.3).

In Bezug auf die Definition der besonders schützenswerten Personendaten erscheint es nicht befriedigend, ausschliesslich auf Angaben über bestimmte Aspekte abzustellen, da allein diese Angaben nicht zwingend Aufschluss darüber geben, wie intensiv der Eingriff in die Privatsphäre ausfällt; vielmehr ist die Frage nach der Sensibilität von Daten häufig auch davon abhängig, in welchem Zusammenhang eine bestimmte Angabe steht: Je nach dessen Ausgestaltung können auch auf den ersten Blick sehr „harmlose" Daten besonders schützenswert sein, so dass darüber nachgedacht werden sollte, wie diese Definition so modifiziert werden kann, dass sie auch diesem Aspekt Rechnung tragen kann. Auch dieser Aspekt wird derzeit im Rahmen der bevorstehenden Revision der Datenschutzkonvention des Europarates sowie der Revision des EU-Datenschutzrechts diskutiert (vgl. Ziffer 15.3).

15.2.6 Zur Sensibilisierung der Betroffenen

Die Bevölkerungsbefragung lieferte Hinweise, dass den Betroffenen der Schutz ihrer Persönlichkeitsrechte wichtig ist; gleichzeitig zeigten sich aber Lücken bei der Kenntnis des Rechtswegs und beim Selbstschutz. Die Analyse der Rechtsprechung machte deutlich, dass die Betroffenen die Durchsetzungsrechte kaum in Anspruch nehmen. An dieser Stelle sollen deshalb kurz Massnahmen diskutiert werden, die direkt auf eine Sensibilisierung der Betroffenen zielen. Eine weitergehende Sensibilisierung hätte im Vergleich zu vielen anderen Massnahmen den Vorteil, dass der vorsichtige Umgang mit persönlichen Daten auch bis zu einem gewissen Grad vor intransparen-

ten Bearbeitungen und Bearbeitern im Ausland schützt. Gleichzeitig ist davon auszugehen, dass mit dem Sensibilisierungsgrad der Betroffenen auch der Druck auf die Bearbeiter steigt, Daten rechtskonform zu bearbeiten.

Die Sensibilität der Betroffenen und mithin der Bearbeiter aktiv zu steigern, ist jedoch mit beträchtlichem Aufwand verbunden. Der Bund versucht verschiedentlich, mit gross angelegten Aufklärungskampagnen die Bevölkerung für ein aktuelles Problem zu sensibilisieren und das Verhalten zu ändern (z.B. Verkehrssicherheit, Gesundheit). Solche Massnahmen mögen unter bestimmten Umständen ein gewisses Wirkungspotenzial haben, sind aber jedenfalls mit beträchtlichem Aufwand verbunden, vor allem wenn eine nachhaltige Verhaltensänderung, z.B. in Richtung eines stärkeren Selbstschutzes bewirkt werden soll. Eine solche Wirkung ist erfahrungsgemäss allenfalls mit dauerhaften Kampagnen über mehrere Jahre zu erzielen, wie sie z.B. im Verkehrsbereich üblich sind (vgl. Bonfadelli/Friemel 2008).

Ein vergleichsweise grosses Potenzial dürfte die Sensibilisierung via Multiplikatoren, so z.B. an Schulen, haben. Dies hat der EDÖB erkannt und entsprechende Unterlagen für Schulen zum Thema Internet erstellt. Inwieweit diese auch angewendet werden und der Datenschutz an Schulen thematisiert wird, liegt jedoch primär in der Zuständigkeit der Kantone. Ganz allgemein gilt jedoch, dass ohne eine massive Steigerung des Mitteleinsatzes eine deutlich stärkere Sensibilisierung der Betroffenen nicht erreicht werden kann, und dass die Sensibilität für den Datenschutz stark von der Thematisierung in den Medien abhängt. So kommen etwa Bonfadelli/Friemel (2008: 26) in ihrer Synthese von 32 Evaluationen zu Kampagnen zur Verkehrssicherheit zum Schluss, dass die Medien die wichtigsten Multiplikatoren seien.

15.3 Zur Einbettung der Entwicklung des schweizerischen Datenschutzrechts in den internationalen Kontext

Wie eingangs bemerkt, konnten die unter 15.2. erwähnten Handlungsoptionen lediglich einige Aspekte aufgreifen, die auf der Grundlage der durchgeführten Untersuchung unseres Erachtens diskussionswürdig sein können. Die Auswahl der skizzierten Handlungsoptionen – die, wie ebenfalls eingangs erwähnt, auch keinen Anspruch auf Vollständigkeit erheben können – erklärt sich denn auch in erster Linie vor dem Hintergrund des thematischen Schwerpunkts der Untersuchung, die sich auf bestimmte Aspekte des Datenschutzgesetzes bzw. seiner Anwendung und Wahrnehmung zu konzentrieren hatte. Daneben – und hierauf wurde dann jeweils auch hingewiesen – beruht die Berücksichtigung gewisser Handlungsoptionen aber auch auf dem Umstand, dass diese derzeit auf internationaler bzw. europäischer Ebene vertieft diskutiert werden. Hinzuweisen ist diesbezüglich auf zwei derzeit laufende Reformbestrebungen der für den Datenschutz relevanten rechtlichen Vorgaben auf internationaler bzw. europäischer Ebene, die für die Schweiz von Bedeutung sein werden:

Europarat

Im Rahmen des Europarats sind derzeit Bestrebungen im Gange, die Datenschutzkonvention des Europarates (Nr. 108), der die Schweiz beigetreten ist, zu „modernisieren", (auch) angesichts der Entwicklungen der Informations- und Kommunikationstechnologien, welche das automatische Sammeln und Bearbeiten von grossen Datenmengen einschliesslich persönlicher Daten erlauben, sowie sonstiger Risiken für den Persönlichkeitsschutz durch die Entwicklung neuer Technologien[260]. So hat das Ministerkomitee des Europarats am 10. März 2010 einen Bericht des Beratenden Ausschusses genehmigt, in welchem dieser ein Zusatzprotokoll zur Datenschutzkonvention vorschlägt, und ihn mit der Erarbeitung eines Entwurfs für ein (weiteres) Zusatzprotokoll beauftragt[261]. Ein erster Entwurf des Zusatzprotokolls könnte bis 2012 vorliegen[262].

Ein Schwerpunkt dieser Arbeiten dürfte eine Überprüfung des Begriffs der personenbezogenen Daten (insbesondere im Zusammenhang mit Angaben, die sich direkt nur auf ein Objekt beziehen, mitunter aber gleichwohl Rückschlüsse auf Personen zulassen) und der anderen Definitionen in Art. 2 DSK sein[263]. Geprüft werden auch eine deutlichere Stellung des Verhältnismässigkeitsgrundsatzes im Konventionstext, die Einführung bzw. ausdrückliche Regelung der Rolle der Einwilligung der Betroffenen in eine Datenbearbeitung, die Verstärkung des Zweckbindungsgrundsatzes[264] und die Regelung der Ausnahmen und Beschränkungen[265]. Weiter wird die Definition der besonders sensiblen Daten überprüft[266]. Besonderes Augenmerk wird sodann auf die Datensicherheit gelegt[267]. Verbessert werden sollen weiter die Rechte der Betroffenen (insbesondere über eine entsprechende Verankerung verschiedener Informationsrechte, aber auch eines Widerspruchsrechts und eines Verbots automatisierter Entscheidungen über Personen)[268]. Diskutiert werden auch die Einführung eines Verantwortlichkeitsprinzips und des Prinzips von Privacy by Design (also die Verpflichtung, datenschutzrechtliche Anliegen in jedem Fall sozusagen unter Anwendung einer Art Vorsorge- und Ursprungsprinzip möglichst früh zu berücksichtigen), ein besonderer Schutz für Minderjährige und besondere Arten der Datenverarbeitung, eine Rekursmöglichkeit für juristische Personen, eine Regelung des anwendbaren Rechts beim grenzüberschreitenden Datenverkehr und eine Präzisierung der Stellung der Kontrollbehörden[269].

---

260 Vgl. etwa zu den Gefahren der WiFi-Netze, die letztlich eine unbemerkte Einsicht in die Kommunikation anderer Personen ermöglichen, zur Entwicklung der Geolokalisierungstechniken sowie verschiedener (weiterer) Aspekte der Internetnutzung Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I), novembre 2010, 3 ff.

261 Beschluss des Ministerkomitees von seinem 1079. Treffen vom 10.3.2010, Traktandum 10.2, zugänglich im Internet unter http://www.coe.int/t/dghl/standardsetting/dataprotection/Decisions_en.asp.

262 Vgl. Arbeitsprogramm im Anhang des Berichts des Ausschusses vom September 2009, CM(2009)189, mit dem Beschluss des Ministerkomitees zusammen veröffentlicht (zit. in Fn. 222).

263 Vgl. Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II), T-PD-BUR (2010) 09 (II) PROV, 12 ff., zugänglich im Internet unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/OJ_T-PD-Bureau22(2010)_en%20100930.asp.

264 *Loc. cit.*, 20 ff.

265 *Loc. cit.*, 36 f.

266 *Loc. cit.*, 23 f.

267 *Loc. cit.*, 24 ff.

268 *Loc. cit.*, 28 ff.

269 *Loc. cit.*, 37 ff.

Europäische Union

Mit dem Vertrag von Lissabon wurde in der Europäischen Union einerseits das Recht auf den Schutz personenbezogener Daten in Art. 16 Abs. 1 AEUV und Art. 8 Grundrechtecharta primärrechtlich verankert und andererseits mit Art. 16 Abs. 2 AEUV eine neue Rechtsgrundlage für die einheitliche Regelung des Datenschutzes eingeführt. Ausserdem wurde die frühere Säulen-Struktur der EU aufgehoben. Dies erfordert eine Revision der datenschutzrechtlichen Regelungen im Unionsrechts, die bislang stark von der „Säulenstruktur" des EU-Rechts geprägt waren. Vor diesem Hintergrund veröffentliche die Europäische Kommission am 4. November 2010 ihre datenschutzrechtliche Strategie[270], in der die Kommission – der die Kompetenz zukommt, auf EU-Ebene Rechtsetzungsvorschläge zu unterbreiten – erläutert, dass die wesentlichen Grundsätze der RL 95/46 nach wie vor Gültigkeit haben und insbesondere ihre Technikneutralität beibehalten werden solle. Probleme ortet die Kommission nach einer öffentlichen Konsultation insbesondere bei der Beherrschung der Auswirkungen neuer Technologien, bei der Binnenmarktdimension des Datenschutzes und beim Umgang mit der Globalisierung und der Verbesserung internationaler Datentransfers. Weiter soll der institutionelle Rahmen für die wirksame Durchsetzung der Datenschutzvorschriften verstärkt werden. Vor allem aber soll eine bereichsübergreifende datenschutzrechtliche Regelung geschaffen werden, die für die Datenverarbeitung in sämtlichen Sektoren und Politikbereichen der EU (und damit auch in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen[271]) gilt.

Mit ihrer datenschutzrechtlichen Strategie verfolgt die Kommission im Wesentlichen fünf Ziele: Stärkung der Rechte des Einzelnen, Stärkung der Binnenmarktdimension, Modifikation der Datenschutzvorschriften in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, Verbesserungen in der globalen Dimension des Datenschutzes und eine bessere Durchsetzung der Datenschutzvorschriften durch einen verstärkten institutionellen Rahmen.

Zu diesem Zweck will die Kommission im Jahr 2011 (unter Berücksichtigung der EU-Grundrechtecharta) Rechtsvorschriften vorschlagen. Weiter will sie prüfen, ob die in einzelnen Rechtsakten enthaltenen sektorspezifischen EU-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen langfristig an die neue allgemeine Datenschutzregelung angepasst werden sollten. In einem zweiten Schritt will die Kommission sodann auch Anpassungen anderer Rechtsakte prüfen[272].

Für die Schweiz sind diese Entwicklungen in der EU deshalb von Bedeutung, weil sie durch ihre Assoziierung an „Schengen"[273] und „Dublin"[274] an zahlreiche datenschutzrechtliche Vorgaben

---

[270] Mitteilung der Kommission vom 4.11.2010, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg.

[271] Für die GASP besteht mit Art. 39 EUV i.V.m. Art. 16 Abs. 2 UAbs. 2 AEUV eine separate Rechtsgrundlage für einen Beschluss des Rates.

[272] Mitteilung der Kommission vom 4.11.2010, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg., 21.

[273] Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (SAA), SR 0.362.31.

[274] Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags (DAA), SR 0.142.392.68.

des EU-Rechts gebunden ist und grundsätzlich auch die Weiterentwicklungen dieses Besitzstands zu übernehmen hat. Dies gilt für die RL 95/46 (zumindest, soweit der Anwendungsbereich der beiden genannten Assoziierungsabkommen betroffen ist) und für zahlreiche bereichsspezifische Regelungen.

Diese Skizzierung der derzeit laufenden Diskussion verdeutlicht, dass die meisten der unter 15.2 erwähnten Handlungsoptionen derzeit auch auf der Ebene des Europarates sowie der Europäischen Union diskutiert werden und abzusehen ist, dass zumindest gewisse Elemente Eingang in rechtlich verbindliche Akte (Zusatzprotokoll zum Datenschutzübereinkommen des Europarates und die neuen datenschutzrechtlichen Rechtsakte in der EU) finden werden. Allerdings sind die diesbezüglichen Arbeiten noch nicht so weit fortgeschritten, dass die genauen Konturen dieser neuen Regelungen wirklich absehbar sind. Für die Frage nach dem Handlungsbedarf in der Schweiz bedeutet dies unseres Erachtens zweierlei: Einerseits lohnt es sich, sich auch in der Schweiz bereits jetzt mit den auf internationaler bzw. europäischer Ebene diskutierten (möglichen) Neuerungen zu befassen, um auf den Erlass verbindlicher Rechtsakte optimal vorbereitet zu sein. Andererseits dürfte es ratsam sein, eine Gesetzesrevision dann (rasch) in Angriff zu nehmen, wenn sich die diesbezüglichen Konturen auf internationaler und europäischer Ebene deutlich abzeichnen.

ANHANG

Literaturverzeichnis

Backhaus, Klaus et al. 2000. Multivariate Analysemethoden. Eine anwendungsorientierte Einführung. Berlin: Springer.

Baeriswyl, Bruno 2009. Vom Selbstverständnis der Beauftragten. Wie die europäischen Datenschutzbeauftragten mit Google Street View umgehen. In: digma 2009/3: 108-111.

BAG/EDÖB 2009. Erhebung der datenschutzrechtlichen Situation bei den Krankenversicherern. Bern

Belser, Urs 2006. Art. 11 – Register der Datensammlungen. In: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.). Basler Kommentar Datenschutzgesetz. Basel. Helbing & Lichtenhahn: 167-179.

Bolliger, Christian/ Marius Féraud 2010. Der Austausch von Personendaten zwischen Bundes-, Kantons- und Gemeindebehörden. Bern.

Bonfadelli, Heinz/Friemel, Thomas 2008. Kommunikationskampagnen im Bereich Verkehrssicherheit. Theoretische Grundlagen, Evaluationsbefunde und Toolbox zur Optimierung der Kampagnenpraxis.

Bundesgericht 2003a ff. Bulletin. Neue Artikel. Articles récents. Nr 19/2003 bis Nr. 8/2011.

Bundesgericht 2003 b ff. Bulletin. Neuanschaffungen. Nr. 10/2003 bis Nr. 4/2010.

Bundesrat 1988. Botschaft zum Bundesgesetz über den Datenschutz. BBl 1988 II, 413-534.

Bundesrat 2009. Botschaft über die Genehmigung und die Umsetzung des Notenaustauschs zwischen der Schweiz und der EU betreffend die Übernahme des Rahmenbeschlusses 2008/977/JI vom 27. November 2008 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. 6749- 6786.

Bundesrat 2003a. Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung. BBl 2003 1963-2046.

Bundesrat 2003b. Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung. BBl 2003: 2101-2155.

Bundesrat 2004. Fragen im Zusammenhang mit der Organisation des Datenschutzes innerhalb der Bundesverwaltung Bericht der Geschäftsprüfungskommission des Nationalrates vom 21. November 2003. Stellungnahme des Bundesrates. vom 24. März 2004. BBl 2004: 1431-1436.

Bundesrat 2010. Austausch personenbezogener Daten zwischen Behörden des Bundes und der Kantone. Bericht des Bundesrates in Erfüllung des Postulates Lustenberger 07.3682 vom 5. Oktober 2007 „Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden“ vom 22. Dezember 2010. Bern.

Digma. Zeitschrift für Datenrecht und Informationssicherheit (2001 ff).

Digma 2007. Zeitschrift für Datenrecht und Informationssicherheit. Sonderheft Scoring.

EDÖB 2009. Was muss in einem Bearbeitungsreglement aufgeführt werden? Bern.

EDSB 1994. Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes.

EDSB/EDÖB. Tätigkeitsberichte 2001/2002 bis 2009/2010.

EFK 2007. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Mitteleinsatz für den Datenschutz in der Bundesverwaltung. Bern.

Epiney, Astrid 2006. Datenschutz und „Bilaterale II". Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte. In: Schweizerische Juristen-Zeitung 102/6: 126 ff.

Eurobarometer 2008. Data Protection in the European Union: Citizen's Perceptions. Analytical Report.

Fraunhofer Institut 2008. Privatsphärenschutz in Soziale-Netzwerke-Plattformen. Darmstadt: Fraunhofer Institut für sichere Informations-Technologie SIT.

GPK-N 2003. Fragen im Zusammenhang mit der Organisation des Datenschutzes innerhalb der Bundesverwaltung. Bericht der Geschäftsprüfungskommission des Nationalrates vom 21. November 2003. BBl 2003: 1413-1430.

Huber, Rene 2006. Fünfter Abschnitt: Eidgenössischer Datenschutzbeauftragter. In: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.). Basler Kommentar Datenschutzgesetz. Basel. Helbing & Lichtenhahn: 353-423.

Kommentar 2008. Kommentar zur Vollzugsverordnung vom 14. Juni 1993 (Stand am 1. Januar 2008) zum Bundesgesetz über den Datenschutz (VDSG, RS 235.11).

Langheinrich, Marc/Friedemann Mattern 2002. Wenn der Computer verschwindet: Was Datenschutz und Sicherheit in einer Welt intelligenter Alltagsdinge bedeuten. In: digma – Zeitschrift für Datenrecht und Informationssicherheit 2/3: 138-142.

Mattern, Friedemann 2003. Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Friedemann Mattern (Hrsg.). Total Vernetzt. Heidelberg. Springer Verlag: 1-41.

Mattern, Friedemann/Christian Floerkemeier 2010. Vom Internet der Computer zum Internet der Dinge. In: Informatik-Spektrum 33/2: 107-121.

Maurer-Lambrou, Urs/Andrea Steiner 2006. Zweiter Abschnitt: Allgemeine Datenschutzbestimmungen. In: Urs Maurer-Lambrou und Nedim Peter Vogt. Basler Kommentar Datenschutzgesetz. Basel. Helbing & Lichtenhahn: 77-114.

Menétrey-Savary, Anne-Catherine 2009. Réviser la loi sur la protection des données? In: Astrid Epiney/Patrick Hobi. Die Revision des Datenschutzgesetzes. Zürich. Schulthess: 151-156.

Pauli, Kurt 2006. Art. 7 – Datensicherheit. In: Urs Maurer-Lambrou/Nedim Peter Vogt. Basler Kommentar Datenschutzgesetz. Basel. Helbing & Lichtenhahn: 114-125.

Petersen, Thomas 2010. Die Einstellungen der Deutschen zum Thema Datenschutz. 5. SCHUFA-Datenschutzkolloquium zum Thema „Wer bin ich im Datennetz – und wenn ja, wieviele?", Berlin, 29.9.2010.

Privatim 2009. Datenschutz in der Schweiz. Erste repräsentative Umfrage (Medienmitteilung und PowerPoint-Präsentation). http://www.privatim.ch (3.2.2010).

Radelfinger, Martin 2010. Die Privatsphäre bleibt schützbar. Verhaltensbasierte Datenverwertungen zielen nicht auf das Individuum. NZZ vom 18.11.2010.

Rosenthal, David/Yvonne Jöhri 2008. Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen. Zürich: Schulthess.

Rossnagel, Alexander 2007. Datenschutz in der Welt allgegenwärtigen Rechnens. In: Information Technology 2: 83-90.

Rudin, Beat 2006. Achter Abschnitt: Schlussbestimmungen. In: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.). Basler Kommentar Datenschutzgesetz. Basel. Helbing & Lichtenhahn: 475-515.

Schaar, Peter 2010. Privacy by Design. In: Identity in the Information society. 3/2: 267-274.

Schweizer, Rainer J. 2008. Art. 13 Abs. 2. In: Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.). Die Schweizerische Bundesverfassung. Kommentar, 2. Aufl., Zürich/St. Gallen/Basel/Genf. Dike/Schulthess: 324-334.

Schweizer, Rainer J. 2009. Die Revision des Datenschutzgesetzes: Hintergrund und Überblick. In: Astrid Epiney/Patrick Hobi (Hrsg.). Die Revision des Datenschutzgesetzes. Zürich. Schulthess: 29-54.

SIR 2010. Schweizerisches Institut für Rechtsvergleichung: Gutachten über das Datenschutzrecht in ausgewählten Staaten. Lausanne.

Thür, Hanspeter 2010. Die Privatsphäre im Zeitalter der digitalen Revolution. Bad Ragaz, Referat vom 13. November 2010 anlässlich des ersten Ragazer Herbstgespräches zum Thema „Der digital entmündigte Mensch“.

Wagschal, Uwe 1999. Statistik für Politikwissenschaftler. München. Oldenbourg.

Anhang 1: Interviewpartnerinnen und -partner

Technologieexpertinnen und -experten:

Solange Ghernaouti, Prof. und Dr. Igli Tashi, Université de Lausanne.

Peter Heinzmann, Prof. Hochschule Rapperswil, Technischer Direktor der Firma cnlab Information Technology Research AG.

Albert Kündig, Prof. emeritus ETH Zürich, ehemaliges Mitglied Leistungsausschuss TA-Swiss.

Marc Langheinrich, Prof. Università della Svizzera italiana.

Rechtsexperten:

Alexandre Flückiger, Prof. Université de Genève.

David Rosenthal, Rechtsanwalt Homburger AG, Co-Autor Handkommentar zum Datenschutzgesetz.

Interessenvertreterinnen und -vertreter:

Florence Bettschart, Rechtsanwältin, Fédérations romands des consomateurs.

Jean-Christophe Schwaab, Zentralsekretär Schweizerischer Gewerkschaftsbund.

Datenbearbeiter

11 Interviews mit Vertretern von privaten Unternehmen (8) und von Bundesorganen (3). Diesen Interviewpartnern ist Anonymität zugesichert worden.

EDÖB: Arbeitsweise (zwei Gruppeninterviews):

Pierre-Yves Baumann, Informatik-Koordinator

Jean-Philippe Walter, Stellvertretender Beauftragter

Marc Buntschu, Chef Einheit 2 (Datenschutz)

Kosmas Tsiraktsopoulos, Chef Einheit 1 (Datenschutz)

Joanne Siegenthaler, Juristische Beraterin

EDÖB: Strategie und allgemeine Fragen zum Datenschutz

Hanspeter Thür, EDÖB, und Jean-Philippe Walter, Stellvertretender Beauftragter

Fallstudien: Interviewpartner EDÖB (Einzel- und Gruppengespräche)

Kosmas Tsiraktsopoulos, Chef Einheit 1 (Datenschutz)

Marc Buntschu, Chef Einheit 2 (Datenschutz)

Jürg Dubs, juristischer Berater

Karin Koç, juristische Beraterin

Urs Scherrer, Informatik

Fallstudien: Datenbearbeiter

Im Rahmen der Fallstudien wurden vier Interviews mit Vertretern von privaten Unternehmen und von Bundesorganen durchgeführt. Diesen Interviewpartnern ist Anonymität zugesichert worden.

Anhang 2: Fragebogen der Bevölkerungsumfrage

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	Einführung: Guten Tag, mein Name ist... vom Markt- und Meinungsforschungsinstitut DemoSCOPE in Adligenswil bei Luzern. Wir führen zurzeit eine Bevölkerungsbefragung durch, bei der es um Ihre Erfahrungen mit dem Thema Informationsaustausch geht. Die Umfrage ist im öffentlichen Interesse, d.h. es wird kein kommerzieller Zweck damit verfolgt. Gerne möchten wir auch Sie dazu befragen. Ihr Haushalt ist zufällig ausgewählt worden. Ihre Antworten werden anonym ausgewertet... Das Interview dauert ca. 10 Minuten INT: WENN PERSON WISSEN WILL, WER DER AUFTRAGGEBER DER UMFRAGE IST: VERSPRECHEN, DASS MAN AM ENDE DER STUDIE BEKANNT GIBT UND DER BEFRAGTE AUF WUNSCH DIE DATEN WIEDER LÖSCHEN LASSEN KANN.
SB1	Geschlecht INT: NICHT FRAGEN, SELBST EINSCHÄTZEN, IM ZWEIFELSFALL NACHFRAGEN Männlich .....1 Weiblich.....2
SB2	Alter Darf ich fragen, wie alt Sie sind? Alter in vollendeten Jahren.....ALTER
1	Einstellung / Einstieg Dank Handy und Internet und immer besseren Verkehrsverbindungen gibt es heutzutage vielmehr die Möglichkeiten, sich mit anderen Menschen zu treffen und Informationen auszutauschen als früher. Ganz allgemein gefragt: Freut Sie diese Entwicklung oder macht Ihnen das eher Sorgen? INT: EINE ANTWORT Freut mich .....1 Macht mir eher Sorgen .....2 --- Weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
2	Schützenswerte Arten von Daten Jetzt zähle ich Ihnen verschiedene Arten von Informationen auf. Sagen Sie mir bitte jeweils, ob es für Sie eher wichtig oder eher nicht so wichtig ist, dass diese Angaben über Sie geschützt werden? EDV: ITEMS ROTIEREN INT: VORLESEN! PRO ZEILE EINE ANTWORT - Angaben über Ihren Gesundheitszustand - Angaben über Ihre politische Haltung - Angaben über Ihr Einkommen oder Vermögen - Persönliche Fotos von Ihnen - Adressangaben - Angaben darüber, was Sie einkaufen - Angaben darüber, welche Websites Sie im Internet besucht haben. (Eher) wichtig, dass diese Angaben über mich geschützt werden .....1 (Eher) nicht so wichtig, dass diese Angaben über mich geschützt werden.....2 Weiss nicht ..... 98 Keine Antwort 99
3	Dilemma Dienstleistung vs. Datenschutz Bei Wettbewerben, Kundenkarten oder auch anderen Dienstleistungen muss man zum Mitmachen manchmal weiter gehende Informationen über die eigene Person angeben (z.B. Geburtsdatum, Geschlecht, Beruf oder auch Hobbies). Ist es schon einmal vorgekommen, dass Sie wegen solchen Angaben auf eine Dienstleistung verzichtet haben? INT:ANTWORTEN VORLESEN! EINE ANTWORT Ja, öfter.....1 Ja, gelegentlich .....2 Ja, bisher einmal .....3 Nein, habe aber schon mal überlegt, ob ich verzichten soll.....4 Nein, ist noch nicht vorgekommen und habe auch nicht überlegt, das zu tun .....5 Nein, weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
4	Haltungen zum Datenschutz Die Menschen haben ganz unterschiedliche Haltungen zum Umgang mit Informationen und Daten über ihre eigene Person. Sagen Sie uns bitte bei den folgenden Aussagen jeweils, ob Sie eher zustimmen oder eher ablehnen. EDV: ITEMS ROTIEREN INT: VORLESEN! PRO AUSSAGE EINE ANTWORT - Dass man sich heutzutage mit anderen Menschen fast ständig und grenzenlos austauschen kann, ist eine gute Sache. - Die Vorstellung, wie viele Stellen heute Informationen über uns normale Leute sammeln und auswerten, kann einem Angst machen. - Mit etwas Vorsicht kann man gut selber kontrollieren, dass persönliche Informationen über einem nicht in falsche Hände geraten. - Es ist schwierig, unter Kontrolle zu behalten, was mit den persönlichen Angaben über einem passiert; deshalb muss eine unabhängige Stelle zum Rechten schauen. - Wer nichts Unrechtes gemacht hat, dem kann es egal sein, was Andere über einem erfahren und weiterverbreiten. Stimme eher zu.....1 Lehne eher ab.....2 Weiss nicht ..... 98 Keine Antwort 99
5	Einstellung zu verschiedenen Formen der Informationssammlung Jetzt zähle ich Ihnen ein paar Sachen auf, wo Daten gesammelt resp. veröffentlicht werden. Sagen Sie mir bitte, ob Sie das eher unterstützen oder eher problematisch finden. EDV: ITEMS ROTIEREN/ SPLIT ITEM 2 (JE 500 BEFRAGTE) INT: VORLESEN¨PRO ZEILE EINE ANTWORT - Sammeln von Privatadressen und weiteren Angaben zum Reklame schicken. - Fotos von Strassen und Plätzen im Internet veröffentlichen / SPLIT-ITEM: Fotos von Strassen und Plätzen im Internet veröffentlichen, wenn Personen erkennbar sind. - Öffentliche Strassen und Plätze mit Überwachungskameras filmen. - Wenn andere Leute ohne Ihr Wissen Fotos von Ihnen veröffentlichen, z.B. im Internet Unterstütze das eher .....1 Finde das eher problematisch.....2 Weiss nicht ..... 98 Keine Antwort 99
6	Erfahrungen mit Datenmissbrauch Ist es schon vorgekommen, dass jemand persönliche Angaben von Ihnen gesammelt oder auf eine Art und Weise verwendet hat, wo Sie das Gefühl hatten, das geht nun wirklich nicht, das ist nicht zulässig? Ja.....1 Nein .....2 Weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
7	Missbrauchserlebnis: Details FILTER: ANTWORT JA BEI FRAGE 6 Um welche Art von Daten oder Angaben ist es dabei gegangen? EDV: ITEMS ROTIEREN INT: NUR VORLESEN, WENN KEINE SPONTANNENNUNG! GUT NACHFRAGEN! MEHRERE ANTWORTEN MÖGLICH! Angaben über Ihren Gesundheitszustand .....1 Angaben über Ihre politische Haltung .....2 Angaben über Ihr Einkommen oder Vermögen .....3 Fotos von Ihnen oder Ihren Bekannten und Verwandten.....4 Angaben darüber, zu welchem Zeitpunkt Sie sich an einem bestimmten Ort befunden haben.....5 Adressangaben.....6 Angaben darüber, was Sie einkaufen .....7 Angaben darüber, welche Websites Sie im Internet besucht haben.....8 (NICHT VORLESEN) Anderes .....TEXT Weiss nicht ..... 98 Keine Antwort 99
8	Missbrauchserlebnis: Reaktion FILTER: ANTWORT JA BEI FRAGE 6 Haben Sie danach etwas unternommen, um das Problem zu lösen? EDV: ITEMS 2-8 ROTIEREN INT: NUR VORLESEN, WENN KEINE SPONTANNENNUNG! GUT NACHFRAGEN! MEHRERE ANTWORTEN MÖGLICH! WENN NUR ALLGEMEINE NENNUNG „DATENSCHUTZBEAUFTRAGER" OHNE „KANTON" ODER „BUND": NACHFRAGEN UND ENTSPRECHEND UNTER CODE 4 ODER 5 ABBUCHEN (NICHT VORLESEN) Nein, keine konkreten Schritte .....1 INT: WENN MAN NUR FREUNDE = PRIVAT GEFRAGT ODER DARÜBER GELESEN HAT, Z.B. IM INTERNET Habe mich an die Person, das Unternehmen, die Behörde gewendet, die meine Daten missbraucht hat ..2 Habe mich an die Polizei gewendet.....3 Habe mich an den Datenschutzbeauftragten vom Kanton gewendet .....4 Habe mich an den Datenschutzbeauftragten vom Bund (EDÖB) gewendet.....5 Habe mich an eine Konsumentenschutzorganisation oder einen Ratgeber (z.B. Beobachter) gewendet....6 Ich bin vor Gericht gegangen .....7 Habe mich an einen Anwalt, eine Rechtsberatung gewendet .....8 (NICHT VORLESEN) Habe mich an jemand anderes gewendet (OFFIZIELL) .....TEXT Weiss nicht ..... 98 Keine Antwort 99
9	Missbrauchserlebnis: Abschluss FILTER: ANTWORT JA BEI FRAGE 6

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	Ist dieses Erlebnis auf eine Art und Weise abgeschlossen worden, wo Sie haben akzeptieren können? Ja ..... 1 Nein ..... 2 Noch nicht abgeschlossen ..... 3 Weiss nicht ..... 98 Keine Antwort 99
10. 1	Missbrauchserlebnis: hypothetisch A FILTER: ANTWORT JA BEI FRAGE 6 Gesetzt den Fall, dass Sie noch einmal in eine solche Situation geraten, dass persönliche Daten von Ihnen missbraucht werden. An wen würden Sie sich in einem solchen Fall wenden? EDV: ITEMS 2-8 ROTIEREN INT: NUR VORLESEN, WENN KEINE SPONTANNENNUNG! GUT NACHFRAGEN! MEHRERE ANTWORTEN MÖGLICH! WENN NUR ALLGEMEINE NENNUNG „DATENSCHUTZBEAUFTRAGER" OHNE „KANTON" ODER „BUND": NACHFRAGEN UND ENTSPRECHEND UNTER CODE 4 ODER 5 ABBUCHEN (NICHT VORLESEN) Niemand. ..... 1 An die Person, das Unternehmen, die Behörde, die meine Daten missbraucht hat ..... 2 An die Polizei ..... 3 An den Datenschutzbeauftragten vom Kanton ..... 4 An den Datenschutzbeauftragten vom Bund (EDÖB) ..... 5 An eine Konsumentenschutzorganisation oder einen Ratgeber, (Beobachter,...). ..... 6 An ein Gericht ..... 7 An einen Anwalt, an eine Rechtsberatung ..... 8 (NICHT VORLESEN) Jemand anderes. ..... TEXT Weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
10.2	Missbrauchserlebnis: hypothetisch B FILTER: ANTWORT NEIN BEI FRAGE 6 Gesetzt den Fall, dass Sie einmal in eine solche Situation geraten, dass persönliche Daten von Ihnen missbraucht werden. An wen würden Sie sich in einem solchen Fall wenden? EDV: ITEMS 2-8 ROTIEREN INT: NUR VORLESEN, WENN KEINE SPONTANNENNUNG! GUT NACHFRAGEN! MEHRERE ANTWORTEN MÖGLICH! WENN NUR ALLGEMEINE NENNUNG „DATENSCHUTZBEAUFTRAGER" OHNE „KANTON" ODER „BUND": NACHFRAGEN UND ENTSPRECHEND UNTER CODE 4 ODER 5 ABBUCHEN (NICHT VORLESEN) Niemand. ..... 1 An die Person, das Unternehmen, die Behörde, die meine Daten missbraucht hat ..... 2 An die Polizei ..... 3 An den Datenschutzbeauftragten vom Kanton ..... 4 An den Datenschutzbeauftragten vom Bund (EDÖB) ..... 5 An eine Konsumentenschutzorganisation oder einen Ratgeber, (Beobachter,...). ..... 6 An ein Gericht ..... 7 An einen Anwalt, an eine Rechtsberatung ..... 8 (NICHT VORLESEN) Jemand anderes. ..... TEXT Weiss nicht ..... 98 Keine Antwort 99
11	Bekanntheit des Datenschutzgesetzes Seit 1993 gibt es in der Schweiz ein Datenschutzgesetz. Das legt fest, was Private oder Bundesstellen mit persönlichen Informationen über die Bevölkerung machen dürfen und was nicht. Haben Sie schon davon gehört, dass es ein solches Gesetz gibt oder bisher noch nicht? Schon davon gehört ..... 1 Bisher noch nicht ..... 2 Weiss nicht ..... 98 Keine Antwort 99
12	DSG: Kenntnis Gerichtsweg Stellen Sie sich vor, ein Unternehmen verwendet persönliche Informationen über Sie auf eine Art und Weise, die gegen das Datenschutzgesetz verstossen. Nun fragen Sie sich, ob Sie sich vor Gericht dagegen wehren können. Welche der folgenden Antworten kommt Ihrer Meinung am nächsten? EDV: ITEMS ROTIEREN INT: VORLESEN; EINE ANTWORT Ich müsste mich zuerst informieren, ob ich vor Gericht gehen kann. ..... 1 Nein, ich kann nicht vor Gericht gehen. ..... 2 Ja, ich kann vor Gericht gehen. ..... 3 Weiss nicht ..... 98 Keine Antwort 99
13	Kenntnis EDÖB FILTER: BISHER EDÖB NOCH NICHT ERWÄHNT (FRAGEN 8, 10.1, 10.2)

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	Es gibt in der Schweiz den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), der sich gegen die missbräuchliche Verwendung von Daten einsetzt. Haben Sie schon davon gehört oder bisher noch nicht? INT: VORLESEN, EINE ANTWORT Schon davon gehört .....1 Bisher noch nicht.....2 Weiss nicht ..... 98 Keine Antwort 99
14. 1	DSG: Kenntnis der EDÖB-Funktion Beratung A FILTER: BISHER EDÖB NOCH NICHT ERWÄHNT (FRAGEN 8, 10.1, 10.2) Stellen Sie sich vor, ein Unternehmen verwendet bestimmte Angaben über Ihre Person, und Sie sind unsicher, ob es das überhaupt darf. Nun fragen Sie sich, ob Sie sich jetzt direkt an diesen Eidgenössischen Datenschutzbeauftragten wenden können. Welche der folgenden Antworten kommt Ihrer Meinung am nächsten? EDV: ITEMS ROTIEREN INT: VORLESEN; EINE ANTWORT Ich müsste mich zuerst informieren. .....1 Ja, ich kann mich beraten lassen. .....2 Nein, ich kann mich nicht beraten lassen. .....3 Weiss nicht ..... 98 Keine Antwort 99
14.2	DSG: Kenntnis der EDÖB-Funktion Beratung B FILTER: EDÖB SCHON ERWÄHNT (FRAGEN 8, 10.1, 10.2) Sie haben früher in unserem Gespräch den Eidgenössischen Datenschutzbeauftragten erwähnt. Stellen Sie sich vor, ein Unternehmen verwendet bestimmte Angaben über Ihre Person, und Sie sind unsicher, ob es das überhaupt darf. Nun fragen Sie sich, ob Sie sich jetzt direkt an diesen Eidgenössischen Datenschutzbeauftragten wenden können. Welche der folgenden Antworten kommt Ihrer Meinung am nächsten? EDV: ITEMS ROTIEREN INT: VORLESEN; EINE ANTWORT Ich müsste mich zuerst informieren. .....1 Ja, ich kann mich beraten lassen. .....2 Nein, ich kann mich nicht beraten lassen. .....3 Weiss nicht ..... 98 Keine Antwort 99
15	Internetnutzung Jetzt geht es um Fragen, die sich um das Internet drehen. Sagen Sie uns bitte, wie häufig Sie das Internet nutzen. Würden Sie sagen, Sie nutzen das Internet... INT: VORLESEN! NUR EINE ANTWORT MÖGLICH täglich, fast täglich .....1 mehrmals pro Woche.....2 mehrmals pro Monat.....3

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	mehrmals pro Jahr .....4 seltener .....5 nie.....6 Weiss nicht ..... 98 Keine Antwort 99
16	Internet und Selbstschutz allgemein Wie ist Ihre Erfahrung, kann man im Internet als Einzelner eher gut oder eher schlecht selber bestimmen, welche Informationen über einem selbst für andere frei zugänglich sind und welche nicht? eher gut.....1 eher schlecht .....2 Weiss nicht ..... 98 Keine Antwort 99
17	Internet: Dienstleistungsnutzung FILTER: ANTWORTEN 1-4 BEI FRAGE 15 Im Internet werden verschiedene Dienstleistungen angeboten, zum Beispiel kann man Sachen einkaufen, eine Reise buchen, Zahlungen abwickeln und so weiter. Wie häufig nutzen Sie solche Angebote alles in allem? INT: VORLESEN! EINE ANTWORT regelmässig.....1 gelegentlich .....2 selten .....3 nie.....4 Weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
18.1	Internet: Gründe für Nutzung einer Dienstleistung FILTER: ANTWORTEN 1-3 BEI FRAGE 17 Ob man eine Internet-Dienstleistung nutzt, kann ausser vom Angebot selber noch von anderen Sachen abhängig sein. Sagen Sie mir bitte, inwieweit die folgenden Punkte Einfluss oder keinen Einfluss darauf haben, ob Sie ein Internet-Angebot nutzen. EDV: ITEMS ROTIEREN (AUSSER ITEM 1+2 =FIX) INT: VORLESEN¨PRO ZEILE EINE ANTWORT - Welche Angaben man zu seiner Person machen muss, um die Dienstleistung nutzen zu können. - Ob der Anbieter einem klar informiert, was er mit weitergehenden persönlichen Angaben zur Person, z.B. Alter oder Kreditkartennummer, macht. - Ob andere Internetnutzer diesen Anbieter empfehlen. - Ob der Anbieter ganz allgemein als seriös gilt, einen guten Ruf hat. Hat Einfluss darauf, ob ich ein Angebot nutze .....1 Hat keinen Einfluss darauf, ob ich ein Angebot nutze.....2 Weiss nicht ..... 98 Keine Antwort 99
18.2	Internet: Gründe für Nichtnutzung einer Dienstleistung FILTER: ANTWORT 4 BEI FRAGE 17 Die Leute geben verschiedene Gründe an, warum sie auf solche Internetdienstleistungen verzichten. Nennen Sie mir bitte den Grund, der für Sie am wichtigsten ist. EDV: ITEMS ROTIEREN INT: SPONTANNENNUNG, WENN KEINE ANTWORT, LISTE VORLESEN; NUR EINE ANTWORT MÖGLICH Ich nutze das Internet nur für andere Zwecke / Desinteresse.....1 Ich finde das zu kompliziert. .....2 Ich finde das zu unsicher .....3 Ich muss zu viele persönliche Angaben machen. .....4 (NICHT VORLESEN) Andere. .....TEXT Weiss nicht ..... 98 Keine Antwort 99
19	Internet: Mitgliedschaft in Sozialen Netzwerken FILTER: ANTWORTEN 1-5 BEI FRAGE 15 Es gibt ja auch sogenannte Soziale Netzwerke wie z.B. Facebook, MySpace, oder Xing. Sind sie Mitglied bei einer solchen Plattform? Ja.....1 Nein .....2 Weiss nicht ..... 98 Keine Antwort 99

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
20.1	Internet: Verhalten in Sozialen Netzwerken FILTER: ANTWORTEN JA BEI FRAGE 19 Sagen Sie uns bitte, ob Sie den folgenden Aussagen zum Mitmachen in Sozialen Netzwerken eher zustimmen oder eher nicht zustimmen. EDV: ITEMS ROTIEREN INT: VORLESEN¨PRO ZEILE EINE ANTWORT - Die Informationen, die man austauscht, sind harmlos, da braucht man nicht weiter darauf zu achten, wer sie in die Hände bekommt. - Man kann mit ein paar Einstellungen dafür sorgen, dass nur ein beschränkter Personenkreis persönliche Einträge oder Fotos sehen kann. - Heutzutage kommt man fast nicht mehr darum herum, sich in solchen Netzwerken zu bewegen. - Die Leute denken oft zu wenig drüber nach, was für Informationen und Bilder sie im Netzwerk bekannt geben. Stimme eher zu .....1 Stimme eher nicht zu .....2 Weiss nicht ..... 98 Keine Antwort 99
20.2	Internet: Gründe für Nichtnutzung Sozialer Netzwerke FILTER: ANTWORT NEIN BEI FRAGE 19 Die Leute geben verschiedene Gründe an, warum sie nicht Mitglied bei einem Sozialen Netzwerk sind. Nennen Sie mir bitte den Grund, der für Sie am wichtigsten ist. EDV: ITEMS ROTIEREN INT: SPONTANNENNUNG, WENN KEINE ANTWORT, FOLGENDE LISTE VORLESEN; NUR EINE ANTWORT MÖGLICH Ich nutze das Internet nur für andere Zwecke / Desinteresse .....1 Ich finde das zu kompliziert. .....2 Ich finde das zu unsicher .....3 Ich muss zu viele persönliche Angaben machen. .....4 (NICHT VORLESEN) Anderer Grund. .....TEXT Weiss nicht ..... 98 Keine Antwort 99
21	Internet: Nutzung von Datensicherheits-Technologie allgemein FILTER: ANTWORTEN 1-4 BEI FRAGE 15 Ist auf Ihrem Computer eines oder mehrere Programme installiert, wo Sie vor kriminellen Zugriffen auf Ihre Computer-Daten schützen soll? Ja .....1 Nein .....2 Weiss nicht 98

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	Keine Antwort 99
22	Internet: Nutzung von Datensicherheits-Technologie beim Surfen FILTER: ANTWORTEN 1-4 BEI FRAGE 15 Es gibt ja auch Techniken wie zum Beispiel anonymes Surfen, Verschlüsseln von E-Mails oder Suchanfragen und so weiter, welche verhindern sollen, dass persönliche Daten von Ihnen ohne Ihr Wissen benutzt werden. Wenden Sie auch solche Programme oder Technologien an? Ja .....1 Nein .....2 Weiss nicht ..... 98 Keine Antwort 99
23	Eigenes Verhalten FILTER: ALLE Jetzt habe ich noch eine ganz allgemeine Frage, die sich nicht nur aufs Internet bezieht: Glauben Sie, dass Sie sich selber so gut wie möglich vor Datenmissbrauch schützen, oder sind Sie unsicher, ob Sie diesbezüglich alles machen? Schütze mich so gut wie möglich .....1 Bin unsicher, ob ich alles mache, was möglich ist .....2 (NICHT VORLESEN) Schütze mich kaum, gar nicht .....3 Weiss nicht ..... 98 Keine Antwort 99
	Jetzt haben wir nur noch ein paar Fragen zu rein statistischen Zwecken.
SB3	Höchste abgeschlossene Ausbildungsstufe (einfache Erhebung) Welche Ausbildung haben Sie zuletzt abgeschlossen? INT: SELBST ZUORDNEN. BEI UNKLARHEIT NACHFRAGEN. NICHT ABGESCHLOSSENE AUSBILDUNGEN WERDEN NICHT ERFASST. WENN JEMAND GERADE IN AUSBILDUNG IST, DANN LETZTE ABGESCHLOSSENE AUSBILDUNG ERHEBEN. EDV: ZUSATZINFORMATIONEN ALS HILFE FÜR INTERVIEWER anzeigen. Keine Ausbildung abgeschlossen .....1 (Keine Ausbildung / Primarschule, bis 7 Jahre obligatorische Schule) Obligatorische Schule .....2 (8 oder 9 Jahre obligatorische Schule / Real-, Sekundar-, Bezirks-, Orientierungsschule, Pro-/Untergymnasium, Sonderschule) Diplommittelschule oder Berufsvorbereitende Schule .....3 (2- bis 3-jährige Ausbildung: Diplommittelschule DMS, Fachmittelschule FMS, Verkehrsschule oder ähnliche Ausbildung) Berufslehre, Vollzeit-Berufsschule .....4 (2- bis 4-jährige Ausbildung: Berufslehre, berufliche Grundbildung mit eidg. Fähigkeitszeugnis oder Berufsattest (oder gleichwertig) sowie Anlehre) Maturitätsschule .....5 (Gymnasiale Maturität / Berufs- oder Fach-Maturität) Lehrerseminar .....6 (vorbereitende Ausbildung für Lehrkräfte von Kindergarten, Primarschule, Handarbeit, Hauswirtschaft) Höhere Fach- und Berufsausbildung 7

NR	FRAGEN, ANTWORTKATEGORIEN & ANWEISUNGEN
	(Höhere Berufsbildung mit eidg. Fachausweis / höhere Fachprüfung mit eidg. Diplom oder Meisterdiplom oder gleichwertige Ausbildung) Höhere Fachschule .....8 (Höhere Fachschule (HF) für Technik (bzw. Technikerschule TS) / HF für Wirtschaft (bzw. HKG) oder ähnliche höhere Fachschule (2 Jahre Voll- oder 3 Jahre Teilzeitstudium) Fachhochschule .....9 Universität, Hochschule .....10 (Bachelor - Universität, ETH, Pädagogische Hochschule /Master / Lizentiat / Diplom / Staatsexamen / Postgrad / Doktorat / Habilitation Universität, ETH, Fachhochschule, Pädagogische Hochschule) Weiss nicht ..... 98 Keine Antwort 99
SB4	Erwerbsstatus (Frage 1) Sind Sie voll- oder teilzeit erwerbstätig, arbeitslos, in Ausbildung oder nicht erwerbstätig? Vollzeit.....1 Teilzeit .....2 In Ausbildung .....3 Arbeitslos.....4 Nicht erwerbstätig .....5 Weiss nicht ..... 98 Keine Antwort 99
SB5	Haushaltsgrösse Wie viele Personen – Sie mitgerechnet - leben in Ihrem Haushalt? 1 Person .....1 2 Personen.....2 3 Personen.....3 4 Personen.....4 5 Personen oder mehr .....5 Weiss nicht ..... 98 Keine Antwort 99
SB6	Bruttohaushaltseinkommen Ich möchte Sie noch um eine Angabe zum Haushalteinkommen fragen. Wir erheben das Haushaltseinkommen nur in groben Kategorien und Sie können sicher sein, dass die Angabe von uns nicht weitergegeben und anonymisiert ausgewertet werden. Wie hoch ist das monatliche Brutto-Haushaltseinkommen (INT: BRUTTO = OHNE ABZUG DER STEUERN / VOR STEUERN) von allen Personen, die in Ihrem Haushalt leben. Ich lese Ihnen die Kategorien vor. Unter 5'000 Franken pro Monat .....1 Zwischen 5'000 und unter 7'000 Franken pro Monat .....2 Zwischen 7'000 und unter 9'000 Franken pro Monat .....3 Zwischen 9'000 und unter 12'000 Franken pro Monat .....4 12'000 Franken pro Monat und mehr .....5 Weiss nicht ..... 98 Keine Antwort 99

Anhang 3: Technische Erläuterungen zur Bevölkerungsumfrage

Ausgangslage und Zielsetzung

Im Auftrag des Bundesamtes für Justiz hat das Politikforschungs- und Beratungsbüro Vatter eine Bevölkerungsbefragung in der Deutsch- und Westschweiz sowie im Tessin durchführen lassen, um die Wirksamkeit des Bundesgesetzes über den Datenschutz zu evaluieren. Die Durchführung der Befragung wurde dem Institut Demoscope AG übertragen.

Forschungskonzept

Erhebungsmethode

- Die Interviews sind telefonisch mittels CATI (computer assisted telephone interviewing) aus unseren zentralen Telefonlabors in Adligenswil bei Luzern sowie in Genf durchgeführt worden.

Grundgesamtheit

- Sprachassimilierte Wohnbevölkerung in der Deutsch- und Westschweiz sowie im Tessin ab 15 Jahre.

Stichprobe

- Random Quota: Zufallsauswahl der Haushalte, Auswahl der Zielperson im Haushalt quotiert nach Alter und Geschlecht (interlocked), zusätzlich quotiert nach Wirtschaftsgebiet (WEMF Region 1-5).
- Alterskategorien: 15-34, 35-54, 55-74, 75-99 Jahre.
- Anzahl Interviews total n=1'014 (708 D-CH + 204 W-CH + 102 I-CH) .
- Basis: Strukturdaten Bevölkerung Schweiz gemäss BFS, VZ2000 (Census), jährliche Anpassung der Strukturen / Schlüsselmerkmale gemäss Hochrechnung des BFS (aktueller Stand: 2009).

Fragebogen

- Der Fragebogen wurde vom Büro Vatter konzipiert, von Demoscope ausgearbeitet sowie in mehreren Etappen mit der Begleitgruppe des Bundesamtes für Justiz besprochen. Die Überarbeitung und Korrektur erfolgten durch das Büro Vatter und Demoscope. Mit 18 geschlossenen und 5 offenen (ungestützten) Fragen sowie 5 soziodemografischen Ermittlungen ist der Fragebogen überwiegend strukturiert.
- Die Übersetzung in Französisch und Italienisch ist von Demoscope veranlasst worden. Die übersetzten Fragebogen wurden dem Auftraggeber nochmals zur Überprüfung vorgelegt.

Die Programmierung in allen drei Sprachen sowie die technischen und Qualitätstests erfolgten durch Demoscope.

Feldvorbereitung und Feldarbeit

- Vor dem Feldstart sind 18 Pretest-Interviews in Deutsch durchgeführt worden, um die Verständlichkeit der Fragen sowie den fehlerfreien Ablauf des Interviews zu überprüfen. Für die Feldarbeit sind erfahrene Interviewer und Interviewerinnen eingesetzt und während der gesamten Feldphase permanent betreut worden (Supervision). Sie wurden vor Beginn der Feldarbeit mündlich und schriftlich instruiert und haben jeweils in ihrer Muttersprache deutsch, französisch oder italienisch befragt.

Feldzeit und Interviewdauer

- Die Befragung hat vom 5. bis zum 13. November 2010 stattgefunden. Die durchschnittliche Interviewdauer betrug 14,5 Minuten.

Datenaufbereitung und Berichterstattung

- Die Resultate sind als Rohdaten (gelabeltes SPSS) aufbereitet worden. Die Antworten auf die ungestützten Fragen wurden nicht vercodet; sie sind im Originalwortlaut in den Rohdatensatz integriert.
- Das Reporting zur Umfrage umfasst ausser den Rohdaten eine Randauszählung (Fragebogen mit Zahlenangaben), den vorliegenden Projektbeschrieb (technische Angaben zur Studie) sowie den Fragebogen im Originalwortlaut in Deutsch, Französisch und Italienisch.

Richtlinien

Die Durchführung der Erhebung ist nach den Normen von vsms swiss interview institute® sowie ESOMAR erfolgt.

Anhang 4: Zusammenfassungen der Fallstudien EDÖB

SAKE (Beratung)

Ausgangslage: Das Bundesamt für Statistik erhebt im Rahmen der Schweizerischen Arbeitskräfterehebung die Erwerbsstruktur und das Erwerbsverhaltens der ständigen Wohnbevölkerung in der Schweiz. Seit Oktober 2009 ist die Teilnahme an der von einer privaten Organisation telefonisch durchgeführten Erhebung obligatorisch.

Auslösung: Die erstmalige Antwortpflicht und die Tatsache, dass die Erhebung telefonisch durch ein vom Bundesamt für Statistik (BFS) beauftragtes privates Institut durchgeführt wurde, führten zu Beschwerden beim EDÖB. Auch trat ein kantonaler Datenschutzbeauftragter mit dem Hinweis an den EDÖB heran, dass aus dem Empfehlungsschreiben des BFS nicht klar hervorgehe, ob die Teilnahme obligatorisch sei. Schliesslich begannen die Medien sich für das Thema zu interessieren.

Vorgehen EDÖB: Anders als bei anderen Beratungen ging der EDÖB in diesem Fall auf das BFS zu. Zunächst verfasste der EDÖB eine eigene Standartantwort (Musterbrief) für Anfragen aus der Bevölkerung. Im Weiteren schlug er dem BFS mittels einer Stellungnahme zur besseren Sicherstellung der Authentifizierung vor, mit Hilfe eines Codes im Informationsschreiben den für die Befragung ausgewählten Personen eine effektive Kontrolle zu ermöglichen. Der EDÖB äussert sich gegenüber obligatorischen Erhebungen grundsätzlich kritisch. Daneben fanden als weitere Elemente der Beratungstätigkeit Treffen mit dem BFS resp. E-Mail-Austausch statt, in denen datenschutzrechtliche Aspekte der SAKE erörtert wurden.

Weitere Bemerkungen: Der vorliegende Fall illustriert ausserdem die Doppelrolle des EDÖB als Berater und als Aufsichtsorgan. Aus der Beratung des BFS im Rahmen von SAKE haben sich zwei Sachverhaltsabklärungen ergeben: In einer ersten untersucht der EDÖB generell die Informationsschreiben des Amtes für Befragungen; die zweite Kontrolle bezieht sich auf die Rolle und Pflichten des BFS im Rahmen der Zusammenarbeit mit dem Umfrageinstitut. Auch wenn die beiden Rollen getrennt werden, kann die Doppelrolle dazu führen, dass sich die Zusammenarbeit mit dem Datenbearbeiter im Rahmen einer Beratung konfliktiver wird und dem EDÖB oder Informationen zurückgehalten werden.

Bilanz: Die Beratung des BFS im Rahmen von SAKE ist aus Sicht des EDÖB auch vor dem Hintergrund der Volkszählung 2010 zu beurteilen. Der EDÖB erachtet es diesbezüglich als wichtig, dass er dabei dank dem vorliegenden Fallbeispiel wertvolle Informationen erhalten hat und zudem Kontakte mit den Datenschutzverantwortlichen im BFS knüpfen konnte, die er bei einer Zusammenarbeit in weiteren Fällen als nützlich beurteilt. Im Weiteren erhofft sich der EDÖB, dass durch solche Fälle die Sensibilität bei den Datenbearbeitern gestärkt wird, so dass der Datenschutz innerhalb der Ämter ein höheres Gewicht erhält.

Baubranche (Beratung)

Ausgangslage: Privatfirma X der Baubranche sammelt Dossiers von Qualitäts-Messdaten einer unbestimmten Zahl von Einzelprojekten. Daten stammen von ihr selbst und anderen Lizenznehmern des Verfahrens. Diese Lizenznehmer haben ihren Sitz in der Schweiz und mehreren EU-Staaten. Der Naturwissenschaftler Y analysiert diese Daten im Auftrag gemeinsam mit dieser Privatfirma und den anderen Lizenznehmern. Die Daten werden für die Zertifizierung eines technischen Systems ausgewertet.

Auslösung: In diesem Fall wandte sich der Bearbeiter (Wissenschaftler) zunächst an den kantonalen Datenschutzbeauftragten, der ihn an den EDÖB weiter verwiesen hat. Dort meldete sich der Datenbearbeiter telefonisch und wurde daraufhin gebeten, das datenschutzrechtliche Problem in einem Mail zu schildern. Aus Sicht des Interviewpartners hatte dieser Fall Klärungsbedarf, so dass nicht auf bereits bestehende Informationsprodukte verwiesen werden konnte.

Vorgehen EDÖB: Nach dem Erhalt der notwendigen Informationen per E-Mail wurde der Bearbeiter zu einer Sitzung eingeladen, in der die Fragen beantwortet wurde. Die Ergebnisse dieser Sitzung wurden vom EDÖB in einer schriftlichen Stellungnahme festgehalten und dem Bearbeiter zugestellt. Fälle dieser Art behandelt der EDÖB gemäss eigenen Aussagen rund 20 pro Jahr.

Weitere Bemerkungen: –

Bilanz: Seitens des Bearbeiters wird die rasche und kompetente Beratung durch den EDÖB als positiv festgehalten. Der EDÖB selber bewertet solche kleinere Beratungen von Datenbearbeitern als wichtig: Vom Kontakt mit mittleren und kleinen Firmen profitieren und lernen die Juristen und Informatiker beim EDÖB; sie führen dazu, dass realistische und in der Praxis umsetzbare Lösungsvorschläge (und nicht realitätsfremde Grundsatzdiskussionen) ausgearbeitet werden.

Google Street View (Sachverhaltsabklärung)

Ausgangslage: Mit der Dienstleistung Google Street View bietet Google die Möglichkeit an, sich im Internet virtuell durch Städte und Dörfer zu bewegen. Dazu nimmt Google Bilder auf, die anschliessend mit einer Anonymisierungssoftware bearbeitet und im Internet publiziert werden. Der EDÖB hatte sich vor der Aufschaltung des Dienstes dahingehend geäussert, dass die Datenbearbeitung nicht gegen das DSG verstosse, wenn Gesichter und Autokennzeichen nicht erkennbar sind. Der Dienst wurde in der Schweiz im August 2009 aufgeschaltet.

Auslösung: Im Anschluss an die Aufschaltung des Dienstes prüfte der EDÖB den Dienst und kam zum Schluss, dass Google Street View aus datenschutzrechtlicher Sicht erhebliche Mängel aufweist. Auch haben zahlreiche betroffene Personen beschwert, bei denen die Anonymisierungssoftware zur Unkenntlichmachung von Gesichtern und Nummernschildern nicht oder nicht ausreichend funktioniert hatte.

Vorgehen EDÖB: Nachdem in Gesprächen mit Google keine Einigung erzielt werden konnte, erliess der EDÖB eine Empfehlung an die Adresse des Datenbearbeiters. In der Empfehlung fordert der EDÖB unter anderem eine verbesserte Lösung zur vollständigen Unkenntlichmachung von Gesichtern und Autokennzeichen, die Anonymisierung im Umfeld heikler Einrichtungen wie z.B. Spitäler, die Löschung bestimmter Aufnahmen sowie eine rechtzeitige Information. Ausserdem verlangt der EDÖB, dass keine neuen Bilder von Schweizer Strassen aufgeschaltet werden, bis die Rechtsfragen geklärt sind. Google kam der Empfehlung nach Angaben des EDÖB in den meisten Punkten nicht nach, worauf dieser wir beim Bundesverwaltungsgericht Klage gegen Google, Inc. und die Google Switzerland GmbH eingereicht hat. Im Rahmen von vorsorglichen Massnahmen verlangte der EDÖB zudem, dass keine weiteren in der Schweiz aufgenommenen Bilder aufgeschaltet und hierzulande keine weiteren Kamerafahrten durchgeführt werden. Im Anschluss daran traf der EDÖB mit Google eine Vereinbarung: Für die Dauer des Gerichtsverfahrens werden keine neuen Bilder aus der Schweiz aufgeschaltet. Bei Kamerafahrten werden allfällig betroffene Personen rechtzeitig informiert. Google verpflichtet sich weiter, ein rechtskräftiges schweizerisches Gerichtsurteil zu akzeptieren und auch auf die sich bereits im Ausland befindlichen Bilder aus der Schweiz anzuwenden. Der EDÖB informiert über die jeweiligen Schritte auf seiner Homepage

Weitere Bemerkungen: Aus Sicht des EDÖB bietet der Fall Google Street View verschiedene Schwierigkeiten. Der Fall erweist sich nicht zuletzt wegen dem nun bevorstehenden Gerichtsverfahren als sehr ressourcenintensiv. Kritisch beurteilt wird ebenfalls die Tatsache, dass ein eindeutiger Ansprechpartner auf Seiten von Google fehlt; zwar gibt es mit Google Switzerland einen Bearbeiter in der Schweiz, wichtige Entscheide würden jedoch im Hauptsitz in den USA gefällt. Bezüglich der Informationsbeschaffungsmöglichkeiten wird kritisch angemerkt, dass der EDÖB die Anonymisierungssoftware bislang (vgl. Klageschrift) nicht überprüfen konnte.

Bilanz: Inwiefern sich der EDÖB mit seinem Vorgehen in diesem Fall durchsetzen kann, ist noch offen. Der EDÖB bemerkt, dass im Falle eines Scheiterns vor Gericht immerhin Rechtsklarheit geschaffen werden konnte. Das Instrument der vorsorglichen Massnahme hat sich in diesem Fall als wirksam erwiesen.

Logistep (Sachverhaltsabklärung)

Ausgangslage: Das Schweizer Unternehmen Logistep forscht mit einer eigenen Software im Internet nach Urheberrechtsverletzungen für Musik- und Video-Dateien. Die gesammelten Daten, die namentlich die IP-Adressen umfassen, werden den Inhabern des Urheberrechts, in den meisten Fällen im Ausland, bekannt gegeben. Die Urheberrechtsinhaber reichen Strafklage gegen Unbekannt unter Vorlage der von Logistep erhobenen Daten ein. Sie erhalten im Rahmen des Strafverfahrens Akteneinsicht und beschaffen sich die Adresse des Inhabers der IP-Adresse (der nicht unbedingt mit dem Urheber der Rechtsverletzung identisch ist). In der Folge machen sie vor dem Abschluss des Strafverfahrens ihre zivilrechtlichen Ansprüche in Form von Schadenersatzforderungen geltend.

Auslösung: Auslöser sind in diesem Fall Datenschutzbehörden aus dem benachbarten Ausland, die den EDÖB auf die Praxis des Datenbearbeiters hinweisen. Aus Sicht des EDÖB wäre es unklug gewesen, auf diese Beschwerden nicht zu reagieren, weil es gegenüber den ausländischen Behörden ein falsches Signal gewesen wäre.

Vorgehen EDÖB: Der EDÖB klärt diesen Sachverhalt ab. Nebst der Prüfung, ob die Datenbearbeitung mit den Grundsätzen des DSG im Einklang steht, beschäftigte er sich auch mit der Frage, ob eine überwiegendes privates Interesse eine solche Datenerhebung allenfalls rechtfertige. Zusammenfassend hält der EDÖB fest, dass die gegenwärtige Datenbearbeitung durch das Unternehmen nicht mit dem DSG vereinbar sein und empfiehlt, die Datenbearbeitung einzustellen. Das Unternehmen liess verlauten, dass es die Empfehlung nicht akzeptiert. Der EDÖB legte daraufhin die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vor. In seinem Urteil hielt das BVGer zwar fest, dass IP-Adressen als Personendaten gelten, war aber der Meinung, dass im vorliegenden Fall die Datenbearbeitung durch ein überwiegendes privates Interesse gerechtfertigt werden kann. Gegen diesen Entscheid reichte der EDÖB Beschwerde beim Bundesgericht ein. Dieses verneinte im Gegensatz zum BVGer ein überwiegendes privates Interesse und hiess die Beschwerde gut. Der EDÖB informiert kommentiert

die verschiedenen Schritte dieser Abklärung auf seiner Homepage und im Tätigkeitsbericht.

Weitere Bemerkungen: In diesem Fall verweist der EDÖB auf einen hohen Aufwand, der im Wesentlichen durch den Gerichtsweg entsteht und Ressourcen absorbiert, die an anderen Orten fehlen. Auch gestaltet sich die Zusammenarbeit mit dem Datenbearbeiter als schwierig; die Mittel zur Informationsbeschaffung werden als genügend beurteilt, auch wenn der EDÖB nicht sicher sein kann, ob der Bearbeiter alle relevanten Unterlagen herausgab.

Bilanz: Die Beurteilung des EDÖB in diesem Fall fällt positiv aus. Welche möglichen Wirkung über den Einzelfall hinausgehen (Verwendung von IP-Adressen im Internet; Tätigkeit von Privaten im Internet), könne man erst nach der Publikation des Bger-Urteils abschätzen. Positiv bewertet der EDÖB die Reaktionen aus dem Ausland.

Mitarbeiter-Check (Sachverhaltsabklärung)

Ausgangslage: Mit dem Dienst „Mitarbeiter-Check" wollte eine Kreditauskunftei bonitätsrelevante Informationen an Personalverantwortliche verkaufen. Diese Informationen bieten Unternehmen bei Neuanstellungen oder bei der Beurteilung angestellter Mitarbeiter (z.B. im Hinblick auf eine mögliche Beförderung) Entscheidungsgrundlagen.

Auslösung: Der EDÖB erhielt noch während der Vorbereitungszeit zum Start des Dienstes aufgrund zahlreicher Werbemails, die der Anbieter des Dienstes verschickt hatte, davon Kenntnis. Innert wenigen Tagen gingen zwischen 10 und 20 Anfragen beim EDÖB, was ihn veranlasst, eine Sachverhaltsabklärung einzuleiten.

Vorgehen EDÖB: Der EDÖB hat bereits aufgrund des Werbemails der betroffenen Firma umfangreiche Kenntnisse der Dienstleistung, die er. Er beantragt daraufhin beim Bundesverwaltungsgericht, den Dienst mittels einer provisorischen Massnahme zu untersagen. Der EDÖB begründet diesen Schritt mit der Vielzahl der potenziell betroffenen Personen, den grossen möglichen Nachteilen für die Betroffenen sowie damit, dass ein zentraler Bereich ihres Lebens betroffen ist. Das BVGer hat das Begehren gutgeheissen und das Anbieten des „Mitarbeiter-Checks" für drei Monate untersagt. Ausserdem hat es den EDÖB aufgefordert, innerhalb dieser Frist eine Sachverhaltsabklärung durchzuführen und eine Empfehlung zu erlassen. Noch während der Abklärung erklärte die Kreditauskunftei, dass sie die Dienstleistung nicht anbieten werde.

Weitere Bemerkungen: Der Einsatz der provisorischen Massnahme führte in diesem Fall zu einem raschen Abschluss, da die Firma noch vor der Beendigung der Kontrolle auf die Einführung des Dienstes verzichtet. Allerdings müsse sich der EDÖB ziemlich sicher sein, ein negativer Entscheid des Gerichts hätte eine schlechte Signalwirkung.

Bilanz: Der hatte gemäss den Aussagen des EDÖB eine gewisse Breitenwirkung. Er begründet dies damit, dass sich nach der Gutheissung der provisorischen Massnahme Nachfragen aus dem Arbeitsbereich häuften; der Fall habe eine gewisse Aufmerksamkeit in der Öffentlichkeit erhalten. Es fand keine spezielle Information ähnlicher Firmen statt. Er rechnet damit, dass ähnliche Angebote auftauchen werden; insofern ist die Breitenwirkung gering.

Krankenversicherungen (Sachverhaltsabklärung)

Ausgangslage: Krankenversicherungen bearbeiten im Rahmen ihrer gesetzlich vorgeschriebenen Aufgabenerfüllung besonders schützenswerte Personendaten. Das Aufsichtsorgan für die öffentlichen Krankenversicherungen ist das Bundesamt für Gesundheit (BAG).

Auslösung: Der Datenschutz im Krankenversicherungsbereich steht aufgrund verschiedener Medienberichte und politischen Vorstössen im öffentlichen Fokus. Der EDÖB seinerseits nennt als konkreten Auslöser die Sachverhaltsabklärung bei der CSS-Versicherung, die deutliche Mängel im Datenschutzbereich aufgezeigt hatte. Die Zusammenarbeit mit dem Aufsichtsorgan BAG kann als „window of opportunity" bezeichnet werden: Beide haben ein Interesse daran, den Datenschutz im Krankenversicherungsbereich näher zu untersuchen und so auf den öffentlichen Druck zu reagieren.

Vorgehen EDÖB: Der EDÖB und das BAG führen gemeinsam eine Umfrage zur datenschutzrechtlichen Situation bei 93 Krankenversicherer durch. Ziel der Umfrage ist es, Hinweise auf mögliche Missstände zu liefern, die anschliessend etappenweise weiterverfolgt werden sollen; so konnte im Anschluss an die Erhebung sichergestellt werden, dass die Anmeldepflicht von Datensammlungen eingehalten wird. Darüber hinaus scheint zum jetzigen Zeitpunkt noch wenig umgesetzt worden zu sein. Zumindest angedacht ist die Empfehlung von Kriterien für die Ausgestaltung des Datenschutzes bei Krankenversicherungen, wobei die Zusammenarbeit mit Verbänden (Schweizerische Gesellschaft für Vertrauensärzte, santésuisse) gesucht wird, um die Krankenversicherer stärker und nachhaltig sensibilisieren zu können. Der EDÖB erachtet dieses flächendeckende Vorgehen als erfolgversprechend, da eine Versicherung allein nichts unternehmen wolle.

Weitere Bemerkungen: Beim EDÖB geht man nicht davon aus, dass dieses flächendeckende Vorgehen auch in

anderen Bereichen möglich sei: Dafür fehlen dem EDÖB die Ressourcen und das spezifische Know-how. Auch wird vermutet, dass die Teilnahmebereitschaft an solchen Umfragen klein sein dürfte; im vorliegenden Fall war es in dieser Hinsicht von Vorteil, dass mit dem BAG das Aufsichtsorgan im Boot war. Die Qualität der Antworten beurteilt man beim EDÖB als sehr unterschiedlich.

Bilanz: Insgesamt ist man beim EDÖB mit der Erhebung zufrieden: Man konnte sich ein generelles Bild machen und will nun die wichtigsten Probleme im Datenschutzbereich angehen. Die knappe Ressourcensituation wirkt dabei einschränkend, so dass bislang wenig davon umgesetzt werden konnte. Stärker als in anderen Fällen spürt man seitens des EDÖB eine gewisse Breitenwirkung: Die Sachverhaltsabklärung bei der CSS-Versicherung in Kombination mit der Befragung seien von anderen Kassen zur Kenntnis genommen worden, und hätten diese (möglicherweise) veranlasst, Unterlagen (z.B. Datenschutzkonzept) zu vervollständigen oder einen Datenschutzverantwortlichen einzusetzen. Auch höre man vermehrt den Wunsch, sich zertifizieren zu lassen. Die Gründe sieht man beim EDÖB nicht zuletzt darin, dass man auf Seiten der Versicherer einen Imageschaden vermeiden will.

Bearbeitungsreglement AVAM (Sachverhaltsabklärung)

Ausgangslage: AVAM ist das Informationssystem für die Arbeitsvermittlung und die Arbeitsmarktstatistik des SECO im Rahmen des Vollzugs des Arbeitslosenversicherungsgesetzes (AVIG). Verschiedene Organe des Bundes und der Kantone sowie andere Organisationen haben Zugriff, das ausführliche Angaben über arbeitslose Personen enthält. Die Verordnung zum Datenschutzgesetz verlangt von Bundesämtern unter gewissen Bedingungen, dass sie für eine Datensammlung ein Bearbeitungsreglement erstellen. Bearbeitungsreglemente sind als Teil der technischen und organisatorischen Massnahmen eines Bearbeiters zur Sicherung des Datenschutzes zu sehen.

Auslösung: Der EDÖB kontrolliert jährlich *stichprobenmässig* ungefähr zehn Bearbeitungsreglemente von Bundesorganen oder auch von anderen Bearbeitern. In der Bundesverwaltung kann man aufgrund der bei unterschiedlichen Stellen zirkulierenden Informatik – Projektaufträgen meist erkennen, welche Projekte aus der Sicht des Datenschutzes sensitiv sind. Aufgrund dieser Informationen kann man bei sensitiven Systemen das Bearbeitungsreglement zur Überprüfung verlangen.

Vorgehen EDÖB: Der EDÖB nahm Kontakt mit dem zuständigen Bundesamt (SECO), welches ihm das auf Basis des Musterreglements des EDÖB erstellte Bearbeitungsreglement vorlegte. Der EDÖB kommentierte das Reglement und machte Verbesserungsvorschläge. Gesamthaft gesehen entspricht dieser Falle eher einer Beratung als einer eigentlichen Kontrolle; der EDÖB weist darauf hin, dass eine Empfehlung nur dann in Betracht käme, wenn das Reglement fehlen würde oder substanzielle Mängel erkennbar wären.. Durch die Tatsache, dass das Bearbeitungsreglement eine transparente und zusammenfassende Darstellung des zu beurteilenden Systems erlaubt, ist es für den EDÖB meist nicht sehr aufwändig, sich einen guten Überblick über das System zu verschaffen. Die Kontrolle von Bearbeitungsreglementen wird beim EDÖB meist von einer Person wahrgenommen, die daneben noch weitere Aufgaben ausführt.

Weitere Bemerkungen: Die Kontrolle der zu beurteilenden Systeme kann aufgrund des Bearbeitungsreglementes gemäss Aussagen des EDÖB effizient geschehen. Sehr Detaillierte technische und organisatorische Analysen werden aber aus Zeit- bzw. Aufwandgründen meist nicht durchgeführt. Teilweise gestaltet sich die Zusammenarbeit mit den Ämtern als schwierig.

Bilanz: Ziel des EDÖB ist es u.a., durch die Kontrolle von Bearbeitungsreglementen die zuständigen Bundesorgane zu sensbiliseren, so dass sich diese mit Datenschutzfragen auseinandersetzen und damit ihre Aufgaben im Bereich des Datenschutzes wahrnehmen und somit den EDÖB entlasten. Im Weiteren wird bei vielen Kontrollen als erstes Dokument das Bearbeitungsreglement heraus verlangt, um sich aus der Sicht des Datenschutzes einen Überblick über das System zu verschaffen. Dies gelingt gemäss den Erkenntnissen in diesem Fall nur teilweise: Zwar zwingt ein Bearbeitungsreglement die verantwortlichen Bundesämter dazu, sich mit dem Datenschutz auseinanderzusetzen; darüber hinaus konnten in diesem Fall jedoch direkt keine grosse Wirkungen festgestellt werden (bspw. dass die Datenschutzverantwortlichen in der Bundesverwaltung eine stärkere Rolle einnehmen würden). Zwischen den verschiedenen Verwaltungseinheiten sind Unterschiede erkennbar, je nachdem, wie der Datenschutz organisiert ist.

Soziale Netzwerke (Information)

Ausgangslage: Unter Sozialen Netzwerken versteht man Portale im Internet, in denen sich angemeldete Benutzerinnen und Benutzer treffen, Freundschaften schliessen und Nachrichten, Fotos und Filme untereinander austauschen. Dazu füllt man unter Angabe von mehr oder weniger detaillierten Auskünften über die eigene Person, Vorlieben und Überzeugungen ein persönliches Profil aus. Die im Rahmen von Sozialen Netzwerken entstehenden datenschutzrechtlichen Herausforderungen können aus zwei Gründen als neuartig bezeichnet werden (vgl. Erläuterungen des EDÖB): Erstens werden die genannten persönlichen Informationen von den Benutzern selber und also

mit ihrer eigenen Einwilligung in die Internetprofile geladen. Und zweitens erhalten Privatpersonen einen umfassenden Zugriff auf die Personendaten anderer Privatpersonen. Daraus ergibt sich für die betroffenen Personen eine Reihe von Gefahren.

Auslösung: Folgende Faktoren veranlassten den EDÖB tätig zu werden: Es erreichten ihn sehr viele Anfragen von Betroffenen und Drittpersonen (z.B. Eltern) zu Sozialen Netzwerken, die Zahl der potenzielle betroffenen Personen ist sehr hoch, und es handelt sich um sensible Daten; daneben bestand ein grosses mediales Interesse am Thema und auch die Politik begann sich mit den Sozialen Netzwerken auseinanderzusetzen.

Vorgehen EDÖB: Seitens des EDÖB schätzte man die Voraussetzungen für eine Intervention im Rahmen seiner Aufsichtstätigkeit als kritisch ein: Realistischerweise könne man als schweizerische Datenschutzbehörde nicht viel gegen einen Provider im Ausland unternehmen; die Chancen eines positiven Urteils sowie insbesondere die Frage nach einer allfälligen Rechtsdurchsetzung seien im internationalen Umfeld mit zu grossen Unsicherheiten und einem hohen Ressourceneinsatz verbunden. Entsprechend entschied man sich, zumindest Erläuterungen zu Sozialen Netzwerken zu publizieren. Dabei nutzte man bereits bestehende, internationale Publikationen. Ziel dieses Dokuments ist die Sensibilisierung der Behörden, Provider und User für einen korrekten und datenschutzkonformen Umgang mit Personendaten bei Sozialen Netzwerken.

Der EDÖB bediente in der Folge verschiedene Kanäle, um die erstellten Erläuterungen bekannt zu machen. Einerseits werden Informationsprodukte allgemein im Internet und im Tätigkeitsbericht publiziert; bestimmte Gruppen (Abonnenten des Newsletters, kantonale und internationale Datenschutzbeauftragte sowie Journalisten) wird das Dokument gezielt zugeschickt. Ebenfalls findet eine Veröffentlichung auf der Privacy-Plattform im Internet statt. Andererseits wurde in diesem Fall zusätzlich ein Pressecommuniqué verfasst.

Weitere Bemerkungen: Neben der Publikation der Erläuterungen auf den „traditionellen" Kanälen, versuchte der EDÖB sich bietende Gelegenheiten, um mit der Thematik Soziale Netzwerke und Internet breitere Kreise zu erreichen, zu nutzen. So wählte er am Europäischen Datenschutztag den Schwerpunkt zu diesen Themen und publizierte ein Lehrmittel für die Oberstufe (Budget: 20'000 Franken); daneben ist er bemüht, in zwei grösseren Projekten der Bundesverwaltung zum Thema Jugendliche und Internet seine Informationen einzubringen bzw. hat dies bereits getan (BAKOM und BSV).

Bilanz: Die Wirksamkeit der Informationstätigkeit ist schwierig zu beurteilen, da lediglich Einschätzungen zur Nutzung vorliegen. Der EDÖB vermutet gestützt auf die Aufrufung des Dokumentes auf seiner Website und der Nachfragen auf seiner Hotline, dass die Erläuterungen zu den Sozialen Netzwerken stärker genutzt werden als diejenigen im Fall *Mobile Computing*.

Mobile Computing (Information)

Ausgangslage: Heute bestehen durch die Möglichkeiten der Informatik mannigfache Varianten der Datenbearbeitung, die einerseits bequem und effizient sind, anderseits insbesondere bei sensiblen Informationen Fragen der Datensicherheit aufwerfen. Insbesondere durch die Mobilität des modernen Menschen ergeben sich neue Risiken. Es stellt sich insbesondere die Herausforderung, wie bei der mobilen Bearbeitung von sensiblen Personendaten die Vertraulichkeit und Sicherheit gewährleistet werden kann, denn Daten und Anwendungen können im Internet in sogenannten Clouds abgespeichert werden.

Auslösung: In diesem Fall lösten Anfragen, vor allem von Kleinunternehmen, bei denen das technische Knowhow fehlte die Aktivität des EDÖB aus. Auch Fachzeitschriften beschäftigten sich vermehrt mit externen Datenbearbeitungen. Auch ist die Zahl der potenziell betroffenen Personen hoch und es handelt sich um sensible Personendaten.

Vorgehen EDÖB: Beim EDÖB gingen keine konkreten Anzeichen ein, dass ein spezifischer Anbieter gegen das DSG verstossen würde. Insofern stand eine Sachverhaltsabklärung gar nicht zur Diskussion. Infolgedessen entschied sich der EDÖB, auf die verschiedenen Anfragen mit der Publikation von Informationen zu reagieren: Damit kann bei Anfragen auf die im Netz publizierten Informationen verwiesen werden. Er beurteilte das Verfassen eines kurzen Artikels im Rahmen der FAQ als zu wenig umfangreich, um der komplexen Thematik gerecht zu werden; stattdessen wurde ein umfangreicheres Dokument verfasst, dass sich an Privatpersonen richtet. Anders als bei den Erläuterungen zu den Sozialen Netzwerken werden weitere Akteure (Unternehmen, Provider) nicht direkt adressiert. Beim EDÖB begründet man dies mit der Ressourcensituation: Man sei nicht in der Lage gewesen, eine umfassende Abhandlung zur Thematik zu verfassen; man konzentrierte sich auf diejenige Gruppe, welche am stärksten auf die Informationen angewiesen sind. Beim EDÖB beurteilt man die Erläuterungen nicht als abschliessende Auseinandersetzung, was sich neben der Frage nach den Ressourcen auch durch die Funktion der Publikation als Ergänzung zur Beratung begründen lässt.

Der EDÖB bediente in der Folge verschiedene Kanäle, um die erstellten Erläuterungen bekannt zu machen. Einerseits werden Informationsprodukte allgemein im Internet und im Tätigkeitsbericht publiziert; bestimmte Gruppen

(Abonnenten des Newsletters, kantonale und internationale Datenschutzbeauftragte sowie Journalisten) wird das Dokument gezielt zugeschickt. Ebenfalls findet eine Veröffentlichung auf der Privacy-Plattform im Internet statt.

Weitere Bemerkungen: Anders als bei den Sozialen Netzwerken konnten im Rahmen dieser Fallstudie keine Hinweise darauf gefunden werden, dass die Erläuterungen zu Mobile Computing direkt in andere Projekte einfliessen konnten.

Bilanz: Die Wirksamkeit der Informationstätigkeit ist sehr schwierig zu beurteilen, da lediglich Einschätzungen zur Nutzung vorliegen. Der EDÖB vermutet gestützt auf die Aufrufung des Dokumentes auf seiner Website und der Nachfragen auf seiner Hotline, dass die Erläuterungen zu den Sozialen Netzwerken stärker genutzt werden als diejenigen im Fall Mobile Computing.

Leitfaden Überwachung (Information)

Ausgangslage: In dieser Fallstudie geht es um die Rechte und Pflichten, welche sowohl die Arbeitgeber als auch die Arbeitnehmenden im Zusammenhang mit der Überwachung des E-Mail-Verkehrs und der Internetnutzung durch den Arbeitgeber haben. Beim EDÖB stellt man fest, dass das Arbeitsrecht zu derartigen Fragen wenige Bestimmungen enthält; gleichzeitig handelt es sich – nicht zuletzt wegen der hierarchischen Beziehung zwischen Arbeitgeber und –nehmer um einen besonders sensiblen Bereich.

Auslösung: Zum einen kann der Leitfaden Überwachung von E-Mail und Internet am Arbeitsplatz im Kontext weiterer Aktivitäten des EDÖB zum Thema Überwachung am Arbeitsplatz gesehen werden: Der EDÖB hat zu diesem Thema bereits Leitfäden und Merkblätter publiziert sowie Sachverhaltsabklärungen durchgeführt. Zum anderen gab es konkrete Anfragen zur Thematik, zunächst von Arbeitnehmenden, dann aber auch von Arbeitgebern und weiteren Organisationen. Seitens der Arbeitgeber waren die Anfragen häufig dadurch begründet, dass sie sich korrekt verhalten und damit vor allfälligen Beschwerden von Seiten der Arbeitnehmerschaft schützen wollen.

Vorgehen EDÖB: Bei der Erarbeitung des Leitfadens wurden Sitzungen mit verschiedenen Akteuren (z.B. SECO, paritätische Kommission) abgehalten. Der EDÖB publiziert den Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz. In den Gesprächen wurde besonders darauf hingewiesen, dass es wichtig sei, aufgrund der raschen technologischen Entwicklungen den Leitfaden aktuell zu erhalten. Hier erweist sich das Internet (im Gegensatz zur Publikation in Form einer Broschüre) als ideales Medium: Neue Entwicklungen können so rasch aufgenommen werden. Durch die verschiedenen Publikationsformen ist es möglich, die grundlegendsten Überlegungen in den Leitfäden festzuhalten; Präzisierungen und neue Themen können demgegenüber im Rahmen von FAQ oder Merkblätter behandelt werden.

Weitere Bemerkungen: Als besondere Herausforderung wird im Arbeitsbereich (wie andernorts auch) die Datenweitergabe ins Ausland betrachtet; dabei stossen nationalstaatliche Regelungen an ihre Grenzen. Ähnlich wie bei der Anmeldung von Datensammlungen vermutet man beim EDÖB auch in diesem Bereich, dass es einen Teil von Bearbeitern gibt, welche diesen Pflichten nicht nachkommen.

Bilanz: Über die Nutzung resp. die Wirksamkeit des Leitfadens können keine genauen Angaben gemacht werden. Aufgrund einzelner Mitteilungen von privaten Datenbearbeitern und gestützt auf die Aufrufung des Dokumentes auf seiner Website und der Nachfragen auf seiner Hotline lässt sich festhalten, dass die Leitfäden genutzt und als qualitativ gut bewertet werden. Es kann nicht davon ausgegangen werden, dass die Leitfäden flächendeckend verwendet werden. Falls sie genutzt werden, wird ihnen durchaus eine gewisse Bedeutung zugesprochen, auch wenn Leitfaden nicht keine Verbindlichkeit haben.

Anhang 5: Mitglieder der Arbeitsgruppe Evaluation DSG

Dr. Martin Hilti	Bundesamt für Justiz, Leitung der Arbeitsgruppe
Dr. Jean-Philippe Walter	EDÖB
Dr. Nadja Braun	Interdepartementale Arbeitsgruppe Datenschutz
Jacques Beglinger	Verein Unternehmensdatenschutz
Dr. Bruno Baeriswyl	Privatim
Thomas Pletscher	Economiesuisse
Jacques Vifian	Eidgenössisches Büro für Konsumentenfragen
Sébastien Fanti	Coutaz et Fanti Avocats et Notaires, Sion
Prof. Dr. Bertil Cottier	Universität Lugano
Rolf Reinhard	Datenschutz-, Öffentlichkeits- und Informationsschutzbeauftragter EJPD
Dr. Werner Bussmann	Bundesamt für Justiz