UNIVERSITAS FRIBURGENSIS
droit / recht
INSTITUT FÜR EUROPARECHT / INSTITUT DE DROIT EUROPEEN

Astrid Epiney / Tamara Civitella /
Patrizia Zbinden

Datenschutzrecht in der Schweiz

Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben

Erstellt im Auftrag des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

2009

Cahiers fribourgeois de droit européen no 10
Freiburger Schriften zum Europarecht Nr. 10

Cahiers fribourgeois de droit européen

Freiburger Schriften zum Europarecht

Publiés sous l'égide de l'Institut de droit européen de l'Université de Fribourg

Herausgegeben vom Institut für Europarecht der Universität Freiburg i. Ü.

Derniers numéros parus / Letzte erschienene Nummern

(http://www.unifr.ch/euroinstitut/n/de/Publikationen/cahiers_de.php)

6 Andrea Faeh

Blut und Blutbestandteile im europäischen und schweizerischen Recht – ein Vergleich der Rechtslage

7 Andrea Faeh

Arzneimittelwerbung im europäischen und schweizerischen Recht – Konvergenzen und Divergenzen der Rechtslage

8 Astrid Epiney / Patrizia Zbinden

Arbeitnehmerentsendung und Freizügigkeitsabkommen Schweiz - EG : Zur Tragweite und Auslegung der Dienstleistungsfreiheit im Freizügigkeitsabkommen Schweiz – EG

9 Sarah Volknandt

Der Vertrag von Lissabon : Vom Verfassungsvertrag zum Reformvertrag – eine Gegenüberstellung ausgewählter Aspekte beider Verträge

10 Astrid Epiney / Tamara Civitella / Patrizia Zbinden

Datenschutzrecht in der Schweiz : Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben

Astrid Epiney / Tamara Civitella / Patrizia Zbinden

Datenschutzrecht in der Schweiz

Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben

L'Institut de droit européen, dirigé par les Professeurs Marc Amstutz, Samantha Besson et Astrid Epiney, contribue, en tant que centre de compétence des Facultés de droit des Universités de Berne, Neuchâtel et Fribourg, à ce que les ressources des trois universités dans ce domaine soient utilisées le plus efficacement possible. Ses activités englobent, hormis les tâches relatives à l'enseignement du droit européen, la gestion d'une bibliothèque et d'un centre de documentation européenne, l'organisation de manifestations pour la formation continue ainsi que la recherche scientifique en droit européen, des avis de droit et des expertises.

Les Cahiers fribourgeois de droit européen proposent des textes, en français, en allemand, en anglais et en italien, qui, pour différentes raisons, ne se prêtent pas à une publication commerciale, tels que des «papers» de discussion de doctorants, des avis de droit ou des versions écrites de conférences données à l'Université de Fribourg.

Das Institut für Europarecht unter der Leitung von Professor Marc Amstutz und den Professorinnen Samantha Besson und Astrid Epiney hat als Kompetenzzentrum der rechtswissenschaftlichen Fakultäten der Universitäten Bern, Neuenburg und Freiburg unter anderem die Aufgabe, zu der effizienten Nutzung der auf diesem Gebiet zu Verfügung stehenden Ressourcen beizutragen. Neben den mit der Lehre im Europarecht verbundenen Aufgaben zählen zu seinen Aktivitäten die Führung einer europarechtlichen Bibliothek und eines europäischen Dokumentationszentrums, die Organisation von Weiterbildungen sowie die wissenschaftliche Forschung im Europarecht und das Erstellen von Rechtsgutachten.

Die Freiburger Schriften zum Europarecht beinhalten Texte auf Deutsch, Französisch, Englisch und Italienisch, die aus verschiedenen Gründen nicht für eine kommerzielle Veröffentlichung geeignet sind, wie z.B. Diskussionspapiere von Doktoranden, Rechtsgutachten oder schriftliche Fassungen von an der Universität Freiburg gehaltenen Vorträgen.

Editeur / Herausgeber Institut de droit européen / Institut für Europarecht

Avenue de Beauregard 11

CH-1700 Fribourg

euroinstitut@unifr.ch

www.unifr.ch/euroinstitut

November 2009

Inhalt

Vorwort 5

1. Kapitel Grundlagen 7

A. Datenschutzrecht: Zielsetzung und Problematik 7

B Völker- und europarechtliche Vorgaben 9
I. Völkerrechtliche Grundlagen 9
II. Unionsrechtliche Vorgaben 11

C Datenschutz in der Verfassung 17

D Das Datenschutzgesetz des Bundes – Grundlagen 18

2. Kapitel Vorgaben für die Datenbearbeitung durch Bundesorgane 21

A Datenschutzrechtliche Grundsätze 21
I. Vorbemerkungen 21
II. Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 DSG) 22
III. Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) 23
IV. Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG) 24
V. Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG) 26
VI. Grundsatz der Transparenz (Art. 4 Abs. 4 DSG) 27
VII. Grundsatz der Datenrichtigkeit und der Datensicherheit (Art. 5 Abs. 1, 7 DSG) 29

B Datenübermittlung ins Ausland 33
I. Grundsatz (Art. 6 Abs. 1 DSG) 34
II. Ausnahmen (Art. 6 Abs. 2 DSG) 34

C Spezifische Vorgaben für Bundesorgane 37
I. Datenschutzrechtliche Verantwortung (Art. 16, 10a DSG) 38
II. Legalitätsprinzip (Art. 17, 17a, 18 DSG) 39
III. Bekanntgabe von Personendaten (Art. 19 DSG) 46
IV. Spezifische Bearbeitungsformen (Art. 21, 22 DSG) 53

3. Kapitel Rechte Einzelner 55

A Auskunftsrecht 55

B Sonstige Ansprüche 58
I. Berichtigung 58
II. Sperrung der Bekanntgabe 59
III. „Bekanntmachungsansprüche“ 61
IV. Sonstige Ansprüche im Zuge einer widerrechtlichen Bearbeitung 62

4. Kapitel Institutionelle Aspekte 64

A Datenschutz- und Öffentlichkeitsbeauftragter 64

B Datenschutzberater 66

C Datensammlungsregister 68

5. Kapitel Schlussbetrachtung: zu den Herausforderungen des Datenschutzrechts 70

Literatur 72

Materialien 74

Rechtsprechungsverzeichnis 75

A EGMR 75

B EuGH 75

C Bundesgericht 75

D Bundesverwaltungsgericht 76

Verzeichnis nützlicher Links 76

Abkürzungen 77

Vorwort

Datenschutz ist in (fast) allen Bereichen der öffentlich- und privatrechtlichen Tätigkeiten in der einen oder anderen Form relevant. Dieser **„Querschnittscharakter" des Datenschutzrechts** und der datenschutzrechtlichen Vorgaben bringt es mit sich, dass die jeweils geltenden und zu beachtenden Vorgaben häufig insofern vielschichtig sind, als viele, teilweise ineinander greifende Rechtsnormen zu beachten sind. Dabei besteht eine Schwierigkeit für die im beruflichen Alltag mit datenschutzrechtlichen Fragen befassten Personen regelmässig darin, neben den jeweils einschlägigen spezifischen Vorgaben auch den **allgemeinen, bereichsübergreifenden datenschutzrechtlichen Bestimmungen** hinreichend Rechnung zu tragen, die nicht nur grundsätzlich subsidiär heranzuziehen, sondern die auch bei der Auslegung der jeweils zu beachtenden besonderen Vorgaben zu beachten sind. Insofern dürfte die effektive Beachtung datenschutzrechtlicher Vorgaben eine gewisse Vertrautheit nicht nur mit den jeweils für das entsprechende Sachgebiet heranzuziehenden Bestimmungen, sondern auch mit den allgemeinen Grundsätzen des Datenschutzrechts voraussetzen.
Genau hier möchte der vorliegende Band ansetzen: Es geht darum, eine **Einführung in das Datenschutzgesetz des Bundes** zu geben, in dem die erwähnten allgemeinen Grundsätze niedergelegt sind, um es den in der Praxis mit datenschutzrechtlichen Fragen befassten Personen zu ermöglichen, sich die (theoretischen und praktischen) Grundlagen in diesem Bereich anzueignen. Dabei konzentriert sich das Lehrmittel einerseits auf Aspekte, die zum **allgemeinen Verständnis des Datenschutzrechts** unerlässlich sind; andererseits werden diejenigen Bereiche erörtert, die spezifisch für mit der **Datenbearbeitung befasste Bundesorgane** von Bedeutung sind, so dass die datenschutzrechtlichen Vorgaben in Bezug auf Datenbearbeitungen durch Private im Wesentlichen ausgespart werden.

Deutlich werden damit auch die Grenzen der vorliegenden Einführung: Es geht nicht darum, alle datenschutzrechtlichen Vorgaben in den verschiedenen Bereichen im Einzelnen zu bearbeiten und zu berücksichtigen. Dies würde nicht nur den Rahmen dieses Bandes sprengen, sondern wäre auch insofern nicht mit seinen Zielsetzungen vereinbar, als es hier um eine sich grundsätzlich an alle (insbesondere in der Bundesverwaltung) mit datenschutzrechtlichen Problemen befassten Personen richtende Publikation geht.
Der vorliegende Band richtet sich damit in erster Linie an in der Bundesverwaltung tätige Personen, die in der einen oder anderen Form mit Fragen des Datenschutzrechts in Berührung kommen oder sich allgemein für diese Problematik interessieren; obwohl es selbstredend in erster Linie um rechtliche Aspekte geht, soll der Band aber auch für mit Datenschutzrecht befasste Nichtjuristen einen Zugang zu diesem Rechtsgebiet bieten. Seine Zielsetzung kann nach dem Gesagten dahingehend zusammengefasst werden, dass es die wesentlichen Grundsätze und die Systematik des für die Bundesorgane massgeblichen Datenschutzrechts vermittelt, auf deren Grundlage es sodann möglich ist, die für den jeweiligen Bereich ggf. einschlägigen spezifischen datenschutzrechtlichen Vorgaben anzuwenden. Insofern geht es hier darum, Grundlagenkenntnisse (so dass auch allgemein keine Vollständigkeit angestrebt wird) zu vermitteln und das Verständnis für die zur Anwendung kommenden rechtlichen Vorgaben zu erleichtern, um auf diese Weise der praktischen Anwendung datenschutzrechtlicher Grundsätze Vorschub zu leisten.

Damit ergibt sich denn auch der **Aufbau** dieser Einführung: In einem ersten Kapitel sind die Grundlagen des Datenschutzrechts (Gegenstand und Problematik, Verankerung im Völker-, Europa- und Verfassungsrecht sowie ein Überblick über das Datenschutzgesetz des Bundes) zu skizzieren. Der Schwerpunkt wird auf dem zweiten Kapitel liegen, das den Vorgaben für die Datenbearbeitung durch Bundesorgane gewidmet ist und neben den (durchaus allgemein geltenden) datenschutzrechtlichen Prinzipien und den Vorgaben der Datenübermittlung ins Ausland auch die spezifischen Vorgaben für Bundesorgane erörtert. In zwei weiteren Kapiteln geht es um die Rechte der Einzelnen sowie die institutionellen Aspekte, bevor in einem letzten Kapitel einige Gedanken zu den Herausforderungen des Datenschutzrechts formuliert werden.

Im Hinblick auf eine bessere Verständlichkeit und Illustration der allgemeinen, im Gesetz abstrakt formulierten Grundsätze wird immer wieder – häufig im Kleintext – auf konkrete Fallbeispiele Bezug genommen, wobei (soweit sachdienlich und möglich) die Rechtsprechung (insbesondere auf Bundesebene) sowie die Praxis der Bundesbehörden berücksichtigt wird. In diesem Sinn werden einzelnen Kapiteln auch häufig „Leitfälle“ vorangestellt, die dann im weiteren Verlauf des Kapitels gelöst werden.

In Bezug auf Materialen und Nachweise wird im Text selbst, der besseren Lesbarkeit halber, weitgehend auf Literatur- und Materialienhinweise verzichtet; hingegen werden den einzelnen Kapiteln grundsätzlich Literatur- und Materialienhinweise vorangestellt. Diese ermöglichen einerseits eine vertiefte Auseinandersetzung mit der Problematik und verweisen andererseits auch auf die bei der Bearbeitung des jeweiligen Abschnitts herangezogenen Quellen. Soweit in einem Kapitel keine spezifische Literatur herangezogen wird, beruhen die Ausführungen auf den im allgemeinen Literatur-, Materialien- und Rechtsprechungsverzeichnis angeführten Quellen. Diese Verzeichnisse geben auch darüber hinaus weitere Hinweise und erlauben Recherchen zu Einzelfragen.

Der vorliegende Band wurde im Auftrag und in Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erarbeitet. Dem Auftraggeber sei an dieser Stelle sehr herzlich für das entgegengebrachte Vertrauen, die verschiedenen Anregungen im Zusammenhang mit der Erarbeitung dieses Bandes sowie die immer sehr angenehme Zusammenarbeit gedankt.

1. Kapitel Grundlagen

Jede Beschäftigung mit datenschutzrechtlichen Fragen setzt zunächst eine Auseinandersetzung mit einigen Grundfragen des Datenschutzrechts voraus, die einerseits die Thematik des Datenschutzrechts selbst (A.), andererseits die massgeblichen Rechtsgrundlagen im Völker- und Europarecht (B.), in der Verfassung (C.) sowie im Datenschutzgesetz des Bundes (D.) betreffen.

Ziel dieses ersten Kapitels ist es damit zum einen, diese Grundlagen des in der Schweiz geltenden Datenschutzrechts zu erfassen und zu kennen, so dass die zum Zuge kommenden rechtlichen Vorgaben in einen breiteren Kontext eingeordnet werden können. Zum anderen soll die Relevanz der europa- und völkerrechtlichen Vorgaben für die Schweiz und insbesondere die Auslegung des in der Schweiz geltenden Rechts deutlich werden.

A. Datenschutzrecht: Zielsetzung und Problematik

Literatur: EPINEY, in: Epiney/Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz, 1 ff.; EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen, 6 ff.

Obwohl sich erste Ansätze für einen Schutz der Privatsphäre recht weit zurückverfolgen lassen (als „right to privacy“ bis ans Ende des 19. Jahrhunderts), sind die Auswirkungen eines schrankenlosen Umgangs mit personenbezogenen Informationen erst im Lichte von automatisierten Informationssystemen, Telekommunikations- und anderer Techniken einer modernen Informationsgesellschaft virulent geworden. So haben sich die rasch voranschreitenden **technologischen Entwicklungen**, die die **automatisierte Verarbeitung** grosser Informationsmengen erst ermöglichten, als **Motor des Datenschutzrechts** erwiesen, das sich insofern (auch) als technikabhängiges Recht entwickelt hat.

Dabei verfolgt der Datenschutz oder das Recht auf „informationelle Selbstbestimmung“ zwei komplementäre „Interessen“:

- Auf der einen Seite ist der Datenschutz ein Teilgehalt des **Rechts auf Schutz der Privatsphäre und der Persönlichkeit** (vgl. auch noch 1. Kap. B.I.3.a), da dem Einzelnen das vorrangige Recht zukommen muss, über die Zulässigkeit der Verarbeitung ihn betreffender Daten zu entscheiden.

- Auf der anderen Seite stellt Datenschutz auch ein eminent **öffentliches Interesse** dar. Denn ein demokratischer Rechtsstaat kann nur funktionieren, wenn Staat und Private nicht die Befugnis haben, beliebige personenbezogene Daten nach Gutdünken zu erheben und zu verwerten, wird doch damit der Bürger nicht (mehr) als eigenverantwortliche Person, die nach freiem Willen Teil am politischen Willensbildungsprozess hat, wahrgenommen. Insofern ist Datenschutz auch eine Voraussetzung für die Wahrnehmung anderer Freiheiten.

Vor diesem Hintergrund ist die Datenschutzgesetzgebung nicht nur „sinnvoll“, so dass sie aufgrund der gegebenen politischen Mehrheiten verabschiedet, aber auch wieder abgeschafft werden könnte. Vielmehr ist die Datenschutzgesetzgebung als Umsetzung eines völker- und verfassungsrechtlichen Auftrages anzusehen, dem verbindlicher Charakter zukommt und die **nicht grundsätzlich „zur Disposition“ des Gesetzgebers** steht.

Deutlich wird damit aber auch, dass im Schnittpunkt des Datenschutzrechts eine **Vielzahl von potenziell miteinander in Konflikt stehender Interessen** liegt, so dass ein Eingriff in das grundsätzlich bestehende alleinige Recht des Einzelnen, über die Verarbeitung ihn betreffender Daten zu entscheiden, durchaus möglich ist, wobei aber die einschlägigen völker- und verfassungsrechtlichen Vorgaben zu beachten sind (1. Kap. B., C.). Dem **Verhältnismässigkeitsgrundsatz** und der **Abwägung der verschiedenen involvierten Interessen** untereinander kommt dabei eine herausragende Bedeutung zu, wobei immer der **„Kerngehalt" des Persönlichkeitsschutzes** zu beachten ist.

B Völker- und europarechtliche Vorgaben

Literatur: Britz, EuGRZ 2009, 1 ff.; Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, passim; Ehmann, EG-Datenschutzrichtlinie, Kurzkommentar, passim; Epiney/Hobi (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, passim; Epiney, SJZ 2006, 121 ff.; Epiney/Hofstötter/Meier/Theuerkauf, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen, 33 ff.; Epiney/Meier/Egbuna-Joss, Schengen/Dublin, in: Bilaterale Verträge I & II Schweiz – EU, 903 ff. Epiney/Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz, passim; Frenz, EuZW 2009, 6 ff.; Füzesséry Minelli/Brunner, in: Accords bilatéraux II Suisse UE, 425 ff.; Grabenwarter, Europäische Menschenrechtskonvention, 189 ff.; Roßnagel-Burkert, 87 ff.; Roßnagel-Brühann, 132 ff.; Zerdick, RDV 2009, 56 ff.; Zilkens, RDV 2007, 196 ff.

Wie in zahlreichen Rechtsgebieten sind auch im Bereich des Datenschutzrechts eine Reihe von **Vorgaben** bzw. **Grundlagen** zu beachten, die sich auf **völker- und europarechtlicher Ebene** entwickelt haben und die für die **Schweiz jedenfalls von Bedeutung und häufig gar rechtlich verbindlich** sind. Im Folgenden sollen diese kurz umrissen werden, wobei der Akzent auf diejenigen Aspekte gelegt wird, die für die Schweiz relevant sind.

Im Einzelnen kann auf der völkerrechtlichen Ebene (I.) zwischen den Aktivitäten auf der Ebene der Vereinten Nationen (I.1.), der OECD (I.2.) und des Europarates (I.3.) unterschieden werden. Besondere Aufmerksamkeit soll den unionsrechtlichen Vorgaben (II.), die über die „Bilateralen Abkommen" teilweise auch für die Schweiz verbindlich sind, geschenkt werden.

I. Völkerrechtliche Grundlagen

1. Vereinte Nationen

Die Generalversammlung der Vereinten Nationen beschloss am 4.12.1990 **Richtlinien betreffend personenbezogene Daten in automatisierten Dateien** (*Guidelines for the Regulation of Computerized Personal Data Files*, Doc. E/CN.4/1990/72). Den Richtlinien sind allgemeine Grundsätze zu entnehmen, die bei der nationalen Gesetzgebung in den Mitgliedstaaten der Vereinten Nationen berücksichtigt werden sollen; sie sollen aber auch auf die Bearbeitung personenbezogener Daten in Dateien Internationaler Organisationen angewandt werden. Es handelt sich hier allerdings lediglich um nicht bindende Richtlinien mit **Empfehlungscharakter**; im Übrigen bleiben sie teilweise in Bezug auf Präzision und materielle Reichweite hinter den übrigen völker- und europarechtlichen Instrumenten zurück, so dass sie für die Schweiz insgesamt von untergeordneter Bedeutung sein dürften.

2. OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) – der neben den EU-Mitgliedstaaten insbesondere noch die USA, Japan, Kanada, Mexiko, Australien, aber auch die Schweiz angehören – hat früh die Notwendigkeit einer internationalen Regelung des Datenschutzes erkannt, wobei der Hintergrund nicht nur (wohl noch nicht einmal primär) im **Persönlichkeitsschutz** zu sehen war, sondern es eher um die **Sicherstellung eines freien Informationsflusses** ging, damit sich der Datenschutz nicht zu einem Handelshemmnis entwickelt.

Von besonderer Bedeutung sind die am 23.9.1980 vom Rat der OECD erlassenen **Leitlinien für den Schutz der Privatsphäre und grenzüberschreitende Ströme personenbezogener Daten** (OECD-Dokument C (80) 58 final). Diese Leitlinien enthalten neben einigen verfahrensrechtlichen Vorgaben insbesondere materielle Bearbeitungsregeln (so die Grundsätze der Datenqualität, der Zweckbindung, der Verwendungsbeschränkung,

der Transparenz und der Verantwortlichkeit) und Regeln zur grenzüberschreitenden Datenübermittlung.
Auch wenn diese Leitlinien lediglich **Empfehlungscharakter** haben und völkerrechtlich nicht verbindlich sind, haben sie entscheidend zur **Entwicklung des Datenschutzrechts** auf internationaler und nationaler Ebene beigetragen, woran auch ihr mitunter eher rudimentärer Präzisierungsgrad nichts ändert. Für die Schweiz sind diese Richtlinien insbesondere im Hinblick auf ihre Relevanz für aussereuropäische Staaten, insbesondere die USA, von Bedeutung, ist doch grundsätzlich davon auszugehen, dass sich die Mitgliedstaaten der OECD an die Leitlinien halten.

3. Europarat

a) Europäische Menschenrechtskonvention

Fall 1 (vgl. Z v. Finnland, EGMR, Reports 1997-I, 323 ff.):
Z war mit X verheiratet gewesen, die Ehe wurde aber geschieden. X und Z hatten beide AIDS. Gegen X wurde ein Strafverfahren u.a. wegen versuchten Totschlags (Ansteckung mit AIDS) eingeleitet. Z machte von ihrem Zeugnisverweigerungsrecht als Ehefrau Gebrauch. Darüber hinaus rügte sie mehrere Massnahmen der zuständigen Behörden: die gerichtlichen Anordnungen an die Ärzte der Z, im Prozess gegen X gegen den Willen der Z auszusagen, die Beschlagnahme von Z's Krankenakten und Einfügung in die Strafprozessakten gegen X, die Anordnung der Veröffentlichung der Prozessakten mit vollem Namen der Z nach 10 Jahren und die Veröffentlichung von Z's Identität und ihrer Krankheit im Urteil des Berufungsgerichts. Im Verfahren vor dem EMGR stand die Vereinbarkeit dieser Massnahmen mit Art. 8 EMRK zur Debatte.

Datenschutz bzw. das Recht der Einzelnen darauf, dass sie betreffende Daten nicht gespeichert und verwertet, also nicht bearbeitet, werden, ist als spezifischer Ausfluss bzw. **Teilbereich des Rechts auf Achtung der Privatsphäre** (Art. 8 EMRK) zu sehen.

Der Schutzbereich des Art. 8 Abs. 1 EMRK umfasst die Erhebung und Speicherung von Daten einer Person sowie ihre Verarbeitung und Verwertung. Eingeschlossen sind damit auch die Aufnahme in ein Register, eine polizeiliche bzw. hoheitliche Überwachung oder Kommunikation (über Telefon, Mail oder auf dem Postweg). Ein enger Bezug zum Privatleben ist nicht notwendig, so dass auch etwa dienstliche Telefongespräche erfasst werden.

Einschränkungen der Garantie des Art. 8 Abs. 1 EMRK müssen den eng auszulegenden Anforderungen des Art. 8 Abs. 2 EMRK entsprechen (gesetzliche Grundlage, Rechtfertigung aus einer der in Art. 8 Abs. 2 EMRK explizit aufgeführten Gründe sowie Verhältnismässigkeit (hierzu noch 2. Kap. A.IV.).

Der Europäische Gerichtshof für Menschenrechte (EGMR) räumt den Vertragsstaaten zwar regelmässig einen weiten Gestaltungsspielraum hinsichtlich der Legitimität des verfolgten Zwecks ein. Hingegen stellt er an die Ausgestaltung der gesetzlichen Grundlage recht hohe Anforderungen: So muss das den Eingriff erlaubende Gesetz hinreichend bestimmt sein, grundsätzlich Vorkehrungen gegen Datenmissbrauch sowie die Möglichkeit der Betroffenen, Auskunft über die ihn gesammelten Daten zu verlangen, enthalten. Auch hat das Gesetz zu bestimmen, wer welche Daten zu welchem Zweck bearbeiten darf, wie lange die Daten aufbewahrt werden dürfen und auf welche Weise die Einhaltung der Vorgaben kontrolliert wird. Bei sensiblen Daten (wie etwa über den Gesundheitszustand) werden erhöhte Anforderungen gestellt.

Lösung Fall 1 (vgl. Z v. Finnland, EGMR, Reports 1997-I, 323 ff.):
Ein Eingriff in die Privatsphäre ist bei allen erwähnten Massnahmen gegeben, handelt es sich doch um personenbezogene Daten, die das Privatleben der Z betreffen.
Fraglich ist hingegen die Rechtfertigung:
Eine gesetzliche Grundlage lag vor (die einschlägige Strafprozessordnung). Die Eingriffsgründe und die Verhältnismässigkeit sind für die in Frage stehenden Massnahmen getrennt zu prüfen:
- Die Aussagepflicht und die Beschlagnahmung der Akten dienten der Verhinderung bzw. Bestrafung strafbarer Handlungen.
- Die Anordnung der Veröffentlichung der Prozessakten soll Rechte und Freiheiten anderer schützen, weil die Veröffentlichung nach 10 Jahren es der Öffentlichkeit erlaubt, Einsicht in die Strafakten zu nehmen und so das Vertrauen in die Gerichte aufrechterhält.
- Hingegen war für die Veröffentlichung von Daten der Z im Urteil kein legitimer Zweck erkennbar.

In Bezug auf die Verhältnismässigkeit der Massnahmen betonte der Gerichtshof, dass die Veröffentlichung vertraulicher medizinischer Daten (die Tatsache, dass Z HIV-positiv ist) das Privat- und Familienleben, aber auch die soziale und berufliche Situation der betroffenen Person dramatisch beeinflussen könne. Dies könne Personen von der Inanspruchnahme ärztlicher Hilfe abhalten und die allgemeinen Anstrengungen, die HIV-Pandemie einzudämmen, untergraben. Daher sei das Interesse an der Wahrung der Vertraulichkeit solcher Informationen bei der Abwägung, ob der Eingriff im Hinblick auf das angestrebte Ziel verhältnismässig war, sehr hoch zu bewerten. Letzten Endes sah der Gerichtshof jedoch die Beschlagnahme der medizinischen Akten der Z und die Aussagepflicht der Ärzte im Verfahren als verhältnismässig an. Anders verhielt es sich dagegen mit der nach Auffassung des EGMR zu früh angesetzten Zugänglichmachung dieser medizinischen Daten für die Öffentlichkeit und der Veröffentlichung der Identität und des medizinischen Zustands der Klägerin in der Entscheidung des Berufungsgerichts.

b) Datenschutzkonvention des Europarates

Die am 17.9.1980 unterzeichnete und am 1.10.1985 in Kraft getretene und auch durch die Schweiz ratifizierte **Konvention Nr. 108 zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten** formuliert für die Vertragsparteien einen **verbindlichen datenschutzrechtlichen Mindeststandard**. Die zentralen Vorschriften der Konvention enthalten **datenschutzrechtliche Grundprinzipien**, insbesondere die Grundsätze von Treu und Glauben, der Zweckbindung, der Verhältnismässigkeit und der Datenqualität (2. Kapitel), Vorgaben für den grenzüberschreitenden Datenverkehr (3. Kapitel) und die Kooperation der Vertragsparteien (4. Kapitel).
Die Konvention stellte – trotz der Offenheit zahlreicher ihrer Verpflichtungen – einen bedeutenden Schritt hin zur Etablierung eines international verbindlichen Mindeststandards im Bereich des Datenschutzes dar. Zu beachten ist aber auch hier, dass die Konvention – wie schon die OECD-Leitlinien – nicht nur den **Schutz des Einzelnen**, sondern auch den **ungehinderten Datenaustausch** zum Gegenstand hat.
Die Schutzwirkungen der Konvention wurden durch das am 8.11.2001 unterzeichnete und am 1.7.2004 in Kraft getretene **Zusatzprotokoll Nr. 181** verstärkt. Das Protokoll verpflichtet die Vertragsstaaten insbesondere zur Einrichtung unabhängiger nationaler Kontrollstellen (vgl. hierzu auch noch unten 4. Kap. A.) und enthält Vorgaben für die Datenübermittlung an Drittstaaten.

II. Unionsrechtliche Vorgaben

Datenschutzrechtliche Regelungen finden sich in der EU auf verschiedenen Ebenen, wobei ihre inhaltliche Tragweite differiert. Dabei kann zwischen dem Datenschutz als Teil des Schutzes der Privatsphäre und damit als allgemeiner Rechtsgrundsatz (1.), bereichsübergreifenden Regelungen (2.) sowie sektoriellen Regelungen (3.) unterschieden werden, bevor auf die Relevanz der unionsrechtlichen Vorgaben für die Schweiz kurz eingegangen werden soll (4.).

1. „Datenschutz als allgemeiner Rechtsgrundsatz“

Da die Europäische Union die Grundrechte achtet, so wie sie in der Europäischen Menschenrechtskonvention (1. Kap. B.I.3.a) gewährleistet sind (Art. 6 Abs. 2 EUV), gilt das Recht auf Achtung der Privatsphäre entsprechend **Art. 8 EMRK** auch in der Europäischen Union bzw. für die Unionsorgane. Es ist somit als sog. **„allgemeiner Rechtsgrundsatz“** für die **Rechtsetzungstätigkeit der Gemeinschaft und der Union verbindlich**, so dass sich Gemeinschafts- und Unionsorgane bei ihrer Rechtsetzungstätigkeit an die Vorgaben dieses Grundrechts halten müssen. Die Einhaltung dieser Vorgaben kann durch den **Europäischen Gerichtshof** überprüft werden.
Die am 7.12.2000 proklamierte **Europäische Grundrechtecharta** enthält in Art. 8 ein Recht auf Schutz personenbezogener Daten.

Im Einzelnen hat nach dieser Bestimmung jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten; solche Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der Betroffenen oder beruhend auf einer gesetzlichen Grundlage verarbeitet werden. Jeder Person wird das Recht eingeräumt, Auskunft über die sie betreffenden Daten zu erhalten und ggf. die Berichtigung der Daten zu erwirken.

Die Grundrechtecharta hat bis auf weiteres keine unmittelbare Rechtswirkung; mit Inkrafttreten des sog. **Vertrages von Lissabon** („Reformvertrag") wird sie aber durch einen Verweis rechtsverbindlich werden. Allerdings spricht Vieles dafür, dass schon jetzt – neben dem Recht auf Achtung der Privatsphäre und in seiner Tragweite über dieses hinausgehend – auch ein **„Datenschutzgrundrecht"** als allgemeiner Rechtsgrundsatz in der Rechtsprechung des EuGH anerkannt ist (EuGH, Rs. C-101/01, Lindqvist, Slg. 2003, I-12971; EuGH, Rs. 275/06, Promisicae, Urt. v. 29.1.2008), wenn auch seine dogmatischen Konturen (noch) nicht ganz klar sind.

2. Bereichsübergreifende Regelungen

Fall 2 (vgl. EuGH, Rs. C-101/01, Lindqvist, Slg. 2003, I-12971):
Die Schwedin L richtet zu Hause auf ihrem eigenen Computer Internetseiten ein, um den Konfirmanden ihrer Gemeinde den Zugang zu Informationen, die sie möglicherweise benötigen, zu erleichtern. Auf ihren Antrag hin stellt der Webmaster der Kirche eine Verbindung zwischen dieser Seite und der Website der Kirche her.
Die fraglichen Internetseiten enthalten Informationen über Frau L und ihre Arbeitskollegen in der Gemeinde, wobei teilweise der vollständige Name, teilweise nur der Vorname genannt wird. Es werden bei einigen Kollegen die Tätigkeiten und Freizeitbeschäftigungen beschrieben, Familienverhältnisse bekannt gegeben und Telefonnummern angegeben. Bei einer Kollegin wird deren Verletzung am Fuss erwähnt. Die auf der Website erwähnten Personen wurden von dieser weder unterrichtet noch lag ihre Einwilligung vor.
In einem gegen Frau L daraufhin eingeleiteten Strafverfahren wegen Verstosses gegen das einschlägige schwedische, die EG-Datenschutzrichtlinie umsetzende Gesetz, stellten sich auch einige Fragen bezüglich der Auslegung der RL 95/46:

- Liegt im Ausgangsfall eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten vor mit der Folge, dass der Anwendungsbereich der RL 95/46 eröffnet ist?
- Ist eine der Ausnahmebestimmungen des Art. 3 Abs. 2 RL 95/46 anwendbar?
- Betrifft die Information über eine Verletzung am Fuss eine Information über die Gesundheit, so dass der für sensible Daten anwendbare Art. 8 RL 95/46 zur Anwendung kommt?
- Kann beim Aufschalten einer Internetseite eine Übermittlung personenbezogener Daten in einen Drittstaat vorliegen?

Bereichsübergreifende datenschutzrechtliche bzw. datenschutzrelevante Regelungen finden sich bislang ausschliesslich in der sog. „Ersten Säule", also im Rahmen des EG-Vertrages. Von Bedeutung sind hier im Wesentlichen drei Rechtsakte:

- Der Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995 L 281, 31) sind – vor dem Hintergrund der dualistischen Zielsetzung der Richtlinie (einerseits Verwirklichung des freien Datenverkehrs im Binnenmarkt, andererseits Beachtung gewisser datenschutzrechtlicher Grundsätze in den Mitgliedstaaten) – insbesondere eine Reihe durch die Mitgliedstaaten zu beachtender datenschutzrechtlicher Grundsätze, Vorgaben für die Datenübermittlung in andere Mitgliedstaaten und Drittstaaten sowie gewisse Bestimmungen über die datenschutzrechtliche Kontrolle in den Mitgliedstaaten zu entnehmen.

  Der **Anwendungsbereich** der RL 95/46 ist denkbar weit ausgestaltet (ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie Verarbeitung in einer Datei gespeicherter personenbezogener Daten, Art. 3 RL 95/46). Art. 3 Abs. 2 RL 95/46 sind aber auch Einschränkungen des Anwendungsbereichs zu entnehmen. Eine solche Einschränkung liegt insbesondere im Falle der Verarbeitung personenbezogener Daten ausschliesslich zur Ausübung persönlicher oder familiärer Tätigkeiten vor.
  Der RL 95/46 sind verschiedene „Kategorien" an Anforderungen für die Umsetzung zu entnehmen, wobei vier Aspekte von besonderer Bedeutung sein dürften:

- Die Mitgliedstaaten haben sicherzustellen, dass die Verarbeitung personenbezogener Daten zulässig ist, so dass eine Reihe allgemeiner **datenschutzrechtlicher Grundsätze** sowie die spezifischen Anforderungen an jede Verarbeitung im Einzelnen (bei der ein **Verbot der Verarbeitung mit Erlaubnisvorbehalt** zum Zuge kommt) zu beachten sind (Art. 6, 7 RL 95/46); Art. 8 RL 95/46 sind besondere Bestimmungen über sensible Daten zu entnehmen. Art. 15 ff. RL 95/46 enthalten weitere Anforderungen (z.B. gewisse formelle Verarbeitungsbedingungen und Anforderungen an die Übermittlung personenbezogener Daten in Drittländer).
- Art. 10, 11, 12, 14 RL 95/46 regeln die **Rechte der Betroffenen**, wobei zwischen Informationsrechten, Auskunftsrechten, dem Widerspruchsrecht sowie Bestimmungen über Rechtsschutz, Haftung und Sanktionen unterschieden werden kann.
- In Art. 13 Abs. 1 RL 95/46 ist die Möglichkeit vorgesehen, bestimmte Kategorien von sich aus der Richtlinie ergebenden Pflichten bzw. Rechten unter gewissen Voraussetzungen **einzuschränken**.
- Schliesslich sind nach Art. 28 Abs. 1 RL 95/46 eine oder mehrere **Kontrollstellen** vorzusehen, die über die in Art. 28 Abs. 2, 3 RL 95/46 formulierten Befugnisse verfügen, wobei ihnen insbesondere Eingriffsbefugnisse gegenüber den für eine Verarbeitung Verantwortlichen zukommen müssen.

- Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, E-Kommunikations-Datenschutzrichtlinie, ABl. 2002 L 201, 37) konkretisiert und ergänzt die RL 95/46 im Bereich der elektronischen Kommunikation, um einen gleichwertigen Schutz in diesem Gebiet zu gewährleisten, geht aber auch teilweise in ihrer Konzeption über die RL 95/46 hinaus, insbesondere durch die Vermeidung eines Bezugs zu einer identifizierbaren Person.

- Die Richtlinie 2006/24 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden (ABl. 2006 L 105, 54) schreibt die systematische, einheitliche und verdachtsunabhängige Speicherung von Telekommunikationsdaten auf Vorrat (während mindestens sechs Monaten und höchstens zwei Jahren) vor, um auf diese im Einzelfall zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten zugreifen zu können.

  Diese Vorratsdatenspeicherrichtlinie war (und ist) sehr umstritten, dies einerseits aus kompetenzrechtlicher Sicht (eine Kompetenz der EG liege mangels eines hinreichend starken Binnenmarktbezugs nicht vor, gehe es doch um die Strafverfolgung), andererseits wegen ihrer (Un-) Vereinbarkeit mit gemeinschaftlichen Grundrechten. Der EuGH hat die RL 2006/24 jedoch für gemeinschaftsrechtskonform erklärt, wobei er sich nicht zur Grundrechtskompatibilität äusserte (EuGH, Rs. C-301/06, Irland/EP und Rat, Urt. v. 10.2.2009).

Daneben wird durch Art. 286 EGV sichergestellt, dass das EG-Datenschutzrecht auch auf **Organe und Einrichtungen der Gemeinschaft** Anwendung findet, und auf der Grundlage von Art. 286 Abs. 2 EGV wurde mit der **Verordnung 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr** (ABl. 2001 L 8, 1) das Amt des **Europäischen Datenschutzbeauftragten** geschaffen.

Lösung Fall 2 (vgl. EuGH, Rs. C-101/01, Lindqvist, Slg. 2003, I-12971):

- Im Ausgangsfall geht es um Informationen über bestimmte oder bestimmbare natürliche Personen: Die Angabe des Namens, von Telefonnummern, Arbeitsverhältnissen, Freizeitbeschäftigungen etc. ermöglichen eine direkte oder indirekte Identifikation der betroffenen Personen. Diese Daten wurden auch einer Verarbeitung im Sinne des Art. 2 lit. b RL 95/46 unterzogen, da sie auf der Internetseite für eine unbestimmte Zahl von Personen zugänglich gemacht wurden. Die Wiedergabe der Informationen auf einer Internetseite durch das Hochladen dieser Seite auf einen Server sowie die notwendigen Schritte, um diese Seite den mit dem Internet verbundenen Personen zugänglich zu machen, erfolgt zumindest teilweise unter Einsatz von Datenverarbeitungsanlagen und damit in automatisierter Form. Die RL 95/46 ist damit in Anwendung der Art. 3 Abs. 1 RL 95/46 grundsätzlich auf den Ausgangsfall anwendbar.
- An diesem Ergebnis ändern auch die in Art. 3 Abs. 2 RL 95/46 vorgesehenen Ausnahmen nichts: Für die Eröffnung des Anwendungsbereichs der RL 95/46 ist es jedenfalls irrelevant, ob im Einzelfall der freie Verkehr zwischen den Mitgliedstaaten beeinträchtigt wird bzw. ein grenzüberschreitender Bezug vorliegt; hierfür enthält Art. 3 RL 95/46 keine Anhaltspunkte, und im Übrigen wäre der Anwendungsbereich der Richtlinie ansonsten sehr ungewiss. Ehrenamtliche oder religionsgemeinschaftliche Tätigkeiten sind ebenfalls nicht als solche vom Anwendungsbereich der RL 95/46 ausgeschlossen, sondern nur insoweit, als es um eine Datenverarbeitung in Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten geht. Hierunter fallen aber nur Tätigkeiten, die zum Privat- und Familienleben von Einzelpersonen gehören, nicht hingegen eine Verarbeitung personenbezogener Daten zur Veröffentlichung im Internet, da diese impliziert, dass die Daten einer unbeschränkten Anzahl von Personen zugänglich gemacht werden.
- Sensible Daten sind solche über bestimmte persönliche Merkmale, u.a. die Gesundheit. Hierunter sind alle Informationen über die körperliche oder psychische Verfassung zu verstehen, so dass es nicht auf eine irgendwie geartete „Sensibilität der sensiblen Daten" ankommt, eine Abgrenzung, die im Übrigen auch nur sehr schwer zu treffen wäre. Daher ist auch eine Information über eine Verletzung am Fuss als sensibel einzustufen.
- Das Aufschalten einer Internetseite impliziert notwendigerweise einen Zugang zu den auf dieser Seite figurierenden Daten in Drittstaaten. Damit wäre letztlich immer eine Unterbindung des Aufschaltens solcher Seiten notwendig, da in irgendeinem Drittland sicherlich kein angemessenes Datenschutzniveau existiert, so dass die RL 95/46 zu einer allgemeinen Regelung des Internets würde, womit deutlich wird, dass diese Problematik gerade nicht durch die RL 95/46 geregelt werden sollte. Daher liegt im Falle des Aufschaltens einer Internetseite keine Übermittlung personenbezogener Daten in einen Drittstaat im Sinne der RL 95/46 vor.

3. Bereichsspezifische Regelungen

Schliesslich sind dem EU-Recht eine Reihe bereichsspezifischer Vorgaben zu entnehmen. Die für die Schweiz bedeutendsten diesbezüglichen Rechtsakte (abgesehen vom Asylbereich) finden sich im Wesentlichen in der sog. „Dritten Säule", die die **polizeiliche und justizielle Zusammenarbeit in Strafsachen** regelt. So enthalten die verschiedenen spezifischen Zusammenarbeitsformen im Rahmen der Dritten Säule jeweils – soweit dies als notwendig und sinnvoll angesehen wird – für das jeweilige Instrument geltende sektorielle datenschutzrechtliche Bestimmungen. Hintergrund dieser sektoriellen Regelungen gerade in der Dritten Säule ist der Umstand, dass die allgemeinen Bestimmungen der RL 95/46 im Rahmen der polizeilichen Zusammenarbeit keine Anwendung finden, so dass es notwendig war, in den jeweiligen Instrumenten die für sachgerecht erachteten datenschutzrechtlichen Garantien zu verankern. Von besonderer Bedeutung sind die datenschutzrechtlichen Bestimmungen in Bezug auf folgende Regelungsmaterien:

- **Schengener Durchführungsübereinkommen**, das in den Rahmen der EU überführt wurde und in Bezug auf das **Schengener Informationssystem (SIS)** und die **polizeiliche Zusammenarbeit** spezifische Datenschutzbestimmungen enthält;

- **Europol**, das „europäische Polizeiamt", das eigene automatisierte Informationssammlungen betreibt, wobei es hier – im Gegensatz zum SIS – nicht um ein Fahndungs-, sondern um ein Analysesystem geht (vgl. das Europol-

Übereinkommen, ABl. 1995 C 316, 1, Europol soll in naher Zukunft in eine europäische Agentur überführt werden);

- **Eurojust**, eine Dokumentations- und Clearingstelle, die die Koordinierung grenzüberschreitender justizieller Ermittlungen und Strafverfolgungsmassnahmen der Mitgliedstaaten bei der Bekämpfung von Schwerkriminalität erleichtern soll (Beschluss 2002/187, ABl. 2002 L 63, 1);

- das im Rahmen der „Ersten Säule" (also des EG-Vertrages) angesiedelte **Eurodacsystem**, das eine Datenbank für Fingerabdrücke einrichtet, wodurch die effektive Anwendung des sog. Dublin-Systems (wonach nur ein Mitgliedstaat bzw. assoziierter Staat für die Behandlung eines Asylgesuchs zuständig ist) sichergestellt werden soll (VO 2725/2000, „Eurodacverordnung", ABl. 2000 L 316, 1);

- Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der EU (ABl. 2000 C 197, 3) und Rahmenbeschluss über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten (Rahmenbeschluss 2006/960, ABl. 2006 L 386, 89).

Mit dem Rahmenbeschluss 2008/977 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. 2008 L 350, 60) wurde aber auch für die Dritte Säule ein auch inhaltlich der RL 95/46 vergleichbarer allgemeiner Datenschutzrechtsakt erlassen, der für die Verarbeitung personenbezogener Daten, die zwischen den Mitgliedstaaten oder zwischen Mitgliedstaaten und Behörden bzw. Informationssystemen auf EU-Ebene im Rahmen der polizeilichen und justiziellen Zusammenarbeit übermittelt oder bereitgestellt werden, Anwendung findet. Allerdings bleiben die erwähnten Spezialbestimmungen nach wie vor von Bedeutung, da sie insoweit Vorrang beanspruchen, als der Datenaustausch zwischen Mitgliedstaaten oder den Zugang mitgliedstaatlicher Behörden zu den errichteten Informationssystemen geregelt wird und es um Bestimmungen über die Verwendung dieser Daten durch den Empfängermitgliedstaat geht. Der Rahmenbeschluss ist bis zum 27.10.2010 umzusetzen; bis dahin bleiben die erwähnten datenschutzrechtlichen Bestimmungen in jedem einzelnen Rechtsakt vollumfänglich massgeblich.

Im Falle des Inkrafttretens des Lissabonner Vertrages wird die Säulenstruktur aufgelöst werden, so dass dann die Frage zu klären sein wird, ob der genannte Rahmenbeschluss und die EG-Datenschutzrichtlinie in einem Rechtsakt „verschmolzen" werden. Wünschenswert wäre es in jedem Fall, durch die Massgeblichkeit eines „allgemeinen" Datenschutzrechtsakts die Zersplitterung und Uneinheitlichkeit der gewährleisteten Rechte zu mindern, was auch der Rechtssicherheit und damit dem Schutz der Einzelnen zuträglich wäre.

4. Zur Relevanz der unionsrechtlichen Vorgaben für die Schweiz

Mit der Ratifikation der **„Bilateralen II"** – zu denen u.a. die hier in erster Linie relevante **Assoziierungen der Schweiz an „Schengen" und an das „Dublin-System"** gehören – wird die Schweiz auch datenschutzrechtliche Bestimmungen des Unionsrechts zu übernehmen bzw. anzuwenden haben. Hierzu gehören die relevanten **sektoriellen Bestimmungen** insbesondere im Bereich der polizeilichen Zusammenarbeit und Eurodac, aber auch die **EG-Datenschutzrichtlinie (RL 95/46)**.

So ist die RL 95/46 nach Anhang B der Schengenassoziierung – neben vielen anderen gemeinschaftlichen Rechtsakten – von der Schweiz anzuwenden, dies sowohl auf Bundesebene als auch in den Kantonen, die vor diesem Hintergrund im Hinblick auf das Inkrafttreten bzw. Inkraftsetzen der Schengenassoziierung teilweise umfangreiche Modifikationen ihrer Datenschutzgesetzgebung in die Wege leiteten, die insbesondere auch die Errichtung unabhängiger Kontrollbehörden umfassen mussten.

Es ist umstritten, ob sich diese durch die Schengenassoziierung begründete „Anwendungspflicht“ der Datenschutzrichtlinie lediglich auf diejenigen materiellen Bereiche bezieht, die von der Schengen/Dublin-Assoziierung erfasst sind, oder ob die Vorgaben der Richtlinie darüber hinaus in allen von ihrem Anwendungsbereich erfassten Gebieten massgeblich sind, mit der Folge, dass die Schweiz die RL 95/46 im Ergebnis wie ein EU-Mitgliedstaat anzuwenden hätte. Die besseren Gründe sprechen schon aus rechtlicher Sicht, jedenfalls aber aus praktischer Sicht für die zuletzt genannte Ansicht.

Auf der Grundlage der beiden erwähnten Assoziierungsabkommen ist die Schweiz grundsätzlich auch verpflichtet, die **Weiterentwicklungen des relevanten Besitzstandes** zu übernehmen, so dass jede Modifikation derjenigen Rechtsakte, die in den Abkommen aufgeführt sind, sowie diejenigen neuen Rechtsakte, die als Weiterentwicklung von „Schengen“ oder „Dublin“ anzusehen sind (wie etwa der erwähnte Rahmenbeschluss 2008/977 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden), für die Schweiz ebenfalls verbindlich werden.

Diejenigen Rechtsakte, die als Teil des „Schengen“- oder „Dublinbesitzstandes“ anzusehen sind, sind in den Anhängen zu den Assoziierungsabkommen aufgeführt. Bei ihrer Modifikation oder im Falle des Erlasses neuer Rechtsakte, die den Schengen- oder Dublinbesitzstand weiterentwickeln, wird dies jeweils im Rechtsakt selbst vermerkt. Der Schweiz werden die entsprechenden Rechtsakte notifiziert, worauf Fristen in Gang gesetzt werden, innerhalb derjenigen die Schweiz die entsprechenden Rechtsakte übernehmen muss. Diese Fristen erlauben grundsätzlich die Durchführung von möglicherweise notwendigen Referenden. Falls die Schweiz einen Rechtsakt nicht übernimmt, zieht dies grundsätzlich – nach Ablauf einer Frist – die Beendigung des jeweiligen Abkommens nach sich, es sei denn, der Gemischte Ausschuss entscheidet (einstimmig) anders.

C Datenschutz in der Verfassung

Literatur: Auer/Malinverni/Hottelier, Droit constitutionnel suisse, vol. II, 186 ff.; Ehrenzeller/Mastronardi/Schweizer/Vallender-Schweizer, Art. 13; Müller/schefer, Grundrechte in der Schweiz, 160 ff.; Kiener/Kälin, Grundrechte, 158 ff.

Art. 13 BV verankert neben dem Anspruch auf Achtung des Privatlebens (einschliesslich der Wohnung) sowie des Brief-, Post- und Fernmeldeverkehrs auch allgemein einen **Anspruch jeder Person auf „Schutz vor Missbrauch ihrer persönlichen Daten“**.

Damit wird – wie schon in Art. 8 der Grundrechtecharta (1. Kap. B.II.1.) – der Schutz personenbezogener Daten vom Schutz der Privatsphäre losgelöst und unabhängig von dem Vorliegen eines Eingriffs in dieselbe als eigenständiges Schutzgut definiert. Insofern kann man hier von einer zweiten Generation datenschutzrechtlicher Regelungen sprechen, die – im Gegensatz zu der etwa in Art. 8 EMRK zum Ausdruck gekommenen ersten Generation (1. Kap. B.I.3.a) – Datenschutz als eigenständiges Ziel unabhängig von einem Eingriff in die Privatsphäre versteht. Daran schliesst sich die dritte Generation datenschutzrechtlicher Regelungen an, die auch den Schutz von Daten, die nicht einer bestimmten identifizierbaren Person zugeordnet werden können, zum Gegenstand hat, ein Ansatz, der sich bislang insbesondere in der RL 2002/58 (Datenschutzrichtlinie für elektronische Kommunikation, 1. Kap. B.II.2.) niedergeschlagen hat.

Der **Schutzbereich des Art. 13 Abs. 2 BV** umfasst – was in der etwas missglückten Formulierung nicht wirklich zum Ausdruck kommt – tatsächlich ein **Grundrecht auf informationelle Selbstbestimmung**, so dass jeder Umgang mit personenbezogenen Daten erfasst ist. Allerdings kann dieses Grundrecht unter Wahrung der Vorgaben des Art. 36 BV (gesetzliche Grundlage, öffentliches Interesse oder Schutz von Grundrechten Dritter, Verhältnismässigkeit sowie Wahrung des Kerngehalts) eingeschränkt werden.

Damit wird der Datenschutz auf verfassungsrechtlicher Stufe verankert, so dass er – ein wichtiger Aspekt, auf den eingangs bereits hingewiesen wurde (1. Kap. A.) – nur unter den verfassungsrechtlich geregelten Voraussetzungen eingeschränkt werden darf und insofern nicht zur Disposition des Gesetzgebers steht.

D Das Datenschutzgesetz des Bundes – Grundlagen

Literatur: Cottier, Jusletter, 17. Dezember 2007; Drechsler, AJP 2007, 1471 ff.; Epiney/Hofstötter/Meier/Theuerkauf, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen, 221 ff.; Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, passim; Müller-Lambrou/Vogt (Hrsg.), Datenschutzgesetz, Kommentar, passim; Schweizer, in: Epiney/Hobi, Revision des Datenschutzgesetzes, 29 ff.; Wermelinger/Schweri, Jusletter, 3. März 2008; Walter, AJP 1993, 52 ff.

Das **Datenschutzgesetz (DSG)** wurde am 19. Juni 1992 nach eingehender Debatte verabschiedet und trat am **1. Juli 1993**, zeitgleich mit der **Datenschutzverordnung (VDSG)** vom 14. Juni 1993, in Kraft.

Damit nahm die **Entstehung des DSG** mehr als **20 Jahre** in Anspruch: Am 17. März 1971 reichte der damalige Nationalrats *Bussey* eine Motion ein, die den „Erlass einer Gesetzgebung, welche den Bürger und dessen Privatsphäre gegen missbräuchliche Verwendung der Computer schützt, andererseits jedoch eine normale Entwicklung der Verwendung von Datenverarbeitungsanlagen sicherstellen soll“ (AmtlBull NR 1972, 2127), verlangte. Im weiteren Verlauf wurden zunächst im Jahr 1981 bundesinterne Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung (BBl 1981 I 1298) erlassen, bevor sich dann zwei Expertenkommissionen mit der Vorbereitung des Datenschutzgesetzes befassten.

Das Datenschutzgesetz wurde mehrfach **modifiziert**. Die **jüngste Änderung** stammt vom 24. März 2006 und ist am **1. Januar 2008** in Kraft getreten. Hintergrund und Zielsetzung dieser Revision war – neben der Sicherstellung der Kompatibilität des DSG mit dem Zusatzprotokoll zur Europaratskonvention (1. Kap. B.I.3.b) – insbesondere die Erhöhung der Transparenz bei der Erhebung persönlicher Daten (in erster Linie bei sensiblen Daten und bei Persönlichkeitsprofilen), die Ermöglichung (in einer Pilotphase) für die eidgenössischen Behörden, den Zugang zu Datenbanken zu testen (unter Einschluss des *online*-Zugangs) sowie eine Erhöhung des Schutzniveaus beim Zugang, der Benützung und der Kontrolle eidgenössischer Daten, die durch kantonale oder kommunale Behörden bearbeitet werden (vgl. Botschaft DSG, BBl 2003 2101). Daneben wurden einige Aspekte klargestellt und auch bei den allgemeinen Grundsätzen gewisse Modifikationen bzw. Präzisierungen vorgenommen.

Der **Geltungsbereich des Datenschutzgesetzes** erschliesst sich aus Art. 2 DSG in Verbindung mit der Zweckbestimmung von Art. 1 DSG und kann durch folgende Aspekte zusammengefasst werden:

- Geschützt sind gemäss Art. 2 Abs. 1 DSG sowohl **natürliche** als auch **juristische Personen**.

- Das Gesetz regelt sowohl Datenbearbeitungen im privaten Bereich bzw. durch **Privatpersonen** (Art. 2 Abs. 1 lit. a DSG) als auch Bearbeitungen durch **Bundesorgane** (Art. 2 Abs. 1 lit. b DSG). Unter den Begriff „Bundesorgane“ fallen die Bundesverwaltung sowie Personen und Organisationen, die mit öffentlichen Aufgaben des Bundes betraut sind.

  Die Datenbearbeitung durch **kantonale Behörden** fällt indes selbst dann nicht unter das DSG, wenn diese mit dem Vollzug von Bundesrecht betraut sind (Art. 2 Abs. 1 lit. b DSG). Dies erklärt sich durch die in der **Bundesverfassung** vorgesehene **Kompetenzverteilung** zwischen Bund und Kantonen, wonach eine Kompetenz des Bundes nur dann vorliegt, wenn diese ausdrücklich in der Verfassung vorgesehen ist. So kennt die Verfassung keine Bestimmung, die die Aufgabe des Datenschutzes explizit dem Bund zuweist und ihn zu einer umfassenden Regelung des Datenschutzes ermächtigt; gleichwohl kommen dem Bundesgesetzgeber auch in diesem Bereich gewisse Kompetenzen zu, denn er kann immer dann (auch) datenschutzrechtliche Fragen im Rahmen einer Annexkompetenz „mitregeln“, wenn ihm für den betreffenden Bereich eine entsprechende Sachkompetenz zukommt. Insofern stützt sich der Bundesgesetzgeber zum Erlass von Datenschutzrecht auf **Annexkompetenzen zu seinen Sachkompetenzen**, wobei Art. 122 Abs. 1 BV (Zivilrecht), Art. 123 Abs. 1 BV (Strafrecht) sowie die entsprechenden Kompetenzen zum

Erlass von Prozessrecht und Art. 164 Abs. 1 lit. g BV als Kompetenz, Organisation und Verfahren der Bundesbehörden zu regeln, von besonderer Bedeutung sind.

- Das Gesetz gilt grundsätzlich für alle Formen der Datenverwendung (Art. 2 Abs. 1 DSG) und umfasst damit sowohl die **manuelle** als auch die **automatische** Datenbearbeitung.

- Art. 2 Abs. 2 DSG **schränkt** den **sachlichen Geltungsbereich** jedoch bezüglich einzelner Datenkategorien und Bearbeitungsvorgänge **ein**.

  So ist das Gesetz nicht anwendbar auf Daten, die ausschliesslich zum persönlichen Gebrauch verwendet werden, auf Datenverarbeitungen im Rahmen der politischen Beratungen auf Bundesebene, in hängigen Zivil- und Strafprozessen, der internationalen Rechtshilfe sowie in verwaltungsrechtlichen Verfahren ab der zweiten Instanz (Art. 2 Abs. 2 lit. a-c DSG). Ausserdem sind öffentliche Register des Privatrechts und Datenbearbeitungen durch das IKRK vom Datenschutzgesetz ausgenommen (Art. 2 Abs. 2 lit. d, e DSG) bzw. unterstehen speziellen Regelungen.

Die relative Weite des Geltungsbereichs des DSG wird auch durch einen Blick auf die Begriffsdefinitionen in Art. 3 DSG deutlich, der die (auch) für den Geltungsbereich des Gesetzes massgeblichen Begriffe der Daten und der Bearbeitung wie folgt definiert:

- Nach Art. 3 lit. a DSG sind **Personendaten** „alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen".

  Eine **Angabe** ist jede Art von Information, sei sie nun als Tatsachenfeststellung oder als Werturteil abgefasst, wobei sie aber in irgendeiner Form festgehalten sein muss

  Bestimmbar ist eine Person, wenn die jeweilige Information zwar keinen eindeutigen Rückschluss auf die Identität zulässt (etwa durch Nennung des Namens und der Adresse oder durch eine einer Person zugewiesenen Nummer), sondern eine Identifikation aufgrund der gegebenen Informationen möglich ist (z.B.: ein 40-jähriger Angestellter des Bundesamtes für Umwelt, der bereits seit 15 Jahren im Dienst des Amtes steht, drei Kinder hat und hobbymässig auf hohem Niveau Orchestermusik betreibt).

- Der Begriff des **Bearbeitens** umfasst nach Art. 3 lit. e DSG jeden „Umgang mit Personendaten, ungeachtet der angewandten Mittel und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten". Damit werden letztlich „von der Wiege bis zur Bahre" alle Handlungen erfasst, die in irgendeiner Form Personendaten betreffen (können).

  In terminologischer Hinsicht ist darauf hinzuweisen, dass das europäische Unionsrecht in der Regel den Begriff der „Verarbeitung" verwendet, womit aber kein sachlicher Unterschied verbunden sein dürfte.

Das **Datenschutzgesetz** gliedert sich in **acht Abschnitte**:

- Der erste Abschnitt umschreibt **Zweck, Geltungsbereich und Begriffe**; letztere sind teilweise für die inhaltliche Tragweite der Vorgaben des DSG von Bedeutung.

- Im zweiten Abschnitt figurieren die **allgemeinen Datenschutzbestimmungen**, die sowohl für die Bearbeitung durch Private als auch durch Bundesorgane Anwendung finden.

  Neben den datenschutzrechtlichen Grundsätzen (2. Kap. A.) werden hier die grenzüberschreitende Bekanntgabe von Daten (2. Kap. B.), gewisse Rechte Einzelner und ihre möglichen Einschränkungen (3. Kap.), die Datenbearbeitung durch Dritte und Zertifizierungsverfahren geregelt.

- Der dritte Abschnitt ist den besonderen Bestimmungen, die bei der **Bearbeitung von Personendaten durch Private** zu beachten sind, gewidmet, die im vorliegenden Band ausgespart werden (oben Vorwort).
- Im vierten Abschnitt figurieren die bei der **Bearbeitung von Personendaten durch Bundesorgane** spezifisch zu beachtenden Vorgaben (2. Kap. C.).
- Gegenstand des fünften Abschnitts ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (4. Kap. A.).
- Der einen Artikel umfassende sechste Abschnitt betrifft **Rechtsschutzfragen**.
- Im siebten Abschnitt sind **Strafbestimmungen** im Falle des Verstosses gegen bestimmte datenschutzrechtliche Vorgaben enthalten.
- Der achte Abschnitt schliesslich ist den (üblichen) **Schlussbestimmungen** gewidmet.

2. Kapitel Vorgaben für die Datenbearbeitung durch Bundesorgane

Die allgemeinen **datenschutzrechtlichen Vorgaben**, die die **Bundesorgane** zu beachten haben, ergeben sich im Wesentlichen aus dem **Datenschutzgesetz**. Es ist aber jeweils auch danach zu fragen, ob und inwieweit für den betreffenden spezifischen Bereich (zusätzliche) **sektorielle Bestimmungen** einschlägig sind, wobei diese im Rahmen dieses Bandes jedoch – wie eingangs erwähnt – nicht behandelt werden können. Allerdings beruhen auch die speziellen sektoriellen Vorgaben in der Regel auf ähnlichen Grundprinzipien wie das Datenschutzgesetz, so dass dieses jedenfalls bei ihrer Auslegung, häufig aber auch darüber hinaus, subsidiär heranzuziehen ist (vgl. bereits die Bemerkungen im Vorwort).
Die bei einer Datenbearbeitung von den Bundesorganen zu beachtenden Vorgaben können in drei grosse „Kategorien" eingeteilt werden: die (auch allgemein zur Anwendung kommenden) **datenschutzrechtlichen Prinzipien** (A.), die Bestimmungen über die **Datenübermittlung ins Ausland** (B.) sowie die spezifisch für die **Datenbearbeitung durch Bundesorgane** zum Zuge kommenden Vorschriften (C.).

Ziel dieses zweiten Kapitels ist es somit, einen durch praktische Beispiele illustrierten Überblick über diejenigen Anforderungen zu geben, die die Bundesorgane bei der Bearbeitung von Personendaten zu beachten haben und den mit Datenbearbeitungen in der Bundesverwaltung befassten Personen auf diese Weise diejenigen Grundlagen zur Verfügung zu stellen, die sie brauchen, um in ihrem jeweiligen Tätigkeitsbereich den Anforderungen des Datenschutzrechts zu genügen.

A Datenschutzrechtliche Grundsätze

Literatur: Maurer-Lambrou/Vogt-MAURER-LAMBROU/STEINER, Art. 4 DSG; Maurer-Lambrou/Vogt-MAURER-LAMBROU, Art. 5 DSG; Maurer-Lambrou/Vogt-PAULI, Art. 7 DSG; ROSENTHAL/JÖHRI, Handkommentar, Art. 4, 5, 7.

I. Vorbemerkungen

Das Datenschutzrecht beruht auf einer Reihe von **Grundsätzen**, die bereichsübergreifend in allen Konstellationen, in denen Daten bearbeitet werden, zu beachten sind. Sie finden sich im Datenschutzgesetz im zweiten Abschnitt („Allgemeine Datenschutzbestimmungen", Art. 4 ff. DSG).

Im Einzelnen handelt es sich um folgende Grundsätze:

- Grundsatz der Rechtmässigkeit (II.);
- Grundsatz von Treu und Glauben (III.);
- Grundsatz der Verhältnismässigkeit (IV.);
- Grundsatz der Zweckbindung (V.);
- Grundsatz der Transparenz bzw. der Erkennbarkeit (VI.);
- Grundsatz der Datenrichtigkeit und der Datensicherheit (VII.).

Die bei der grenzüberschreitenden Bekanntgabe von Personendaten zu beachtenden Anforderungen (Art. 6 DSG) – die gelegentlich auch als Teil der datenschutzrechtlichen Grundsätze begriffen werden – betreffen letztlich eine besondere Form der Datenbearbeitung (nämlich die Bekanntgabe ins Ausland), so dass es sich weniger um einen allgemeinen datenschutzrechtlichen Grundsatz, denn um in einer besonderen Situation zu beachtende Vorgaben handelt, die daher separat (unten 2. Kap. B.) erörtert werden sollen.

Diese Grundsätze geben die eigentlichen Leitideen des Datenschutzgesetzes wieder (BBl 1988 II 449) und bilden daher letztlich die **Basis des Datenschutzrechts**. Es handelt sich hierbei um **Bearbeitungsgrundsätze**, die beim Bearbeiten von Personendaten eingehalten

werden müssen. Als abstrakt-generelle Grundsätze müssen sie selbstredend auf die sich jeweils stellende Konstellation und den jeweiligen Sachbereich angewandt werden, so dass sie je nach dem betroffenen Bereich unterschiedliche Präzisierungen erfahren können.

Auch wenn im Folgenden an die einschlägigen Regelungen im Datenschutzgesetz des Bundes angeknüpft wird, ist jedoch nicht zu verkennen, dass diese Grundsätze – schon weil sie sich letztlich auch in den einschlägigen völker- und europarechtlichen Vorgaben finden (1. Kap. B.) – ebenfalls in den **kantonalen Datenschutzgesetzen** verankert sind (wenn auch die Formulierungen teilweise divergieren), so dass die folgenden Ausführungen grundsätzlich auch für die Kantone von Bedeutung sind.

Die datenschutzrechtlichen Grundsätze sind für Bundesorgane auch schon deshalb von grundlegender Bedeutung, weil sie als **direkt anwendbares Verhaltensrecht** zu verstehen und damit zu beachten sind (BBl 1988 II 449).

Dabei haben die Bundesorgane darüber hinaus die in Art. 16 ff. DSG verankerten **spezifischen Bestimmungen für Bundesorgane** zu beachten (zu diesen 2. Kap. C.), die teilweise an gewisse datenschutzrechtliche Grundsätze anknüpfen.

Ein Verstoss gegen die hier erörterten Bearbeitungsgrundsätze durch Bundesorgane bei der Bearbeitung von Personendaten ist **keiner Rechtfertigung** zugänglich (insoweit im Gegensatz zur Bearbeitung von Personendaten durch Private, vgl. Art. 13 DSG). Allerdings kann eine **gesetzliche Grundlage**, die Bundesorganen die Bearbeitung von Personendaten erlaubt, selbst gewisse Abweichungen vorsehen; dies stellt jedoch ein Ausfluss des Grundsatzes der Rechtmässigkeit dar.

Ziel des Abschnittes „Datenschutzrechtliche Grundsätze" ist es, einen Überblick über die allgemein gültigen Bearbeitungsgrundsätze zu liefern. Diese sind bei jeder Datenbearbeitung zu beachten und einzuhalten. Sie liefern zudem Anhaltspunkte und Verhaltenshilfen bei der Interpretation der spezifischen datenschutzrechtlichen Regelungen der diversen Bundesorgane.

II. Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 DSG)

Fall 3:
Gestützt auf die Eisenbahnverordnung (EBV, SR 742.141.1) sowie die departementale Verordnung über die Zulassung zum Führen von Triebfahrzeugen der Eisenbahnen (VTE, SR 742.141.142.1) ordnet die SBB die Vornahme von Drogen- und Alkoholtests bei Berufsgattungen mit hohem Sicherheitsaspekt an. Das Eisenbahngesetz (EBG, SR 742.101) enthält keine diesbezüglichen Bestimmungen. Ist dieses Vorhaben aus datenschutzrechtlicher Sicht zulässig?

Nach Art. 4 Abs. 1 DSG dürfen Personendaten nur **rechtmässig bearbeitet** werden. Ein rechtswidriges Verhalten liegt dabei immer schon dann vor, wenn die Bearbeitung der Daten (zum weiten Begriff des Bearbeitens 1. Kap. D.) gegen eine **in der Schweiz geltende rechtlich verbindliche Norm** verstösst. Die Verletzung der in der Schweiz geltenden Rechtsordnung bei der Beschaffung und weiteren Bearbeitung von Personendaten ist damit allgemein unzulässig.

Die (möglicherweise) verletzte Norm kann in **allen geltenden Rechtsnormen** zu finden sein, so z.B. im StGB (Art. 179 ff. StGB), im Obligationenrecht (Täuschung oder Drohung, vgl. Art. 28 f. OR) oder auch im DSG selbst. Besondere Bedeutung kommt dem Grundsatz der Rechtmässigkeit bei der **Beschaffung** von Personendaten zu.
Für **Bundesorgane** ist **Art. 17 DSG** von besonderer **Bedeutung**. Danach dürfen Bundesorgane Personendaten grundsätzlich (zu den Ausnahmen Art. 19, 22 DSG) bearbeiten, wenn sich die Bearbeitung auf eine genügende gesetzliche Grundlage stützt. Zudem ist spezifisch bei der Beschaffung noch Art. 18 DSG zu beachten (2. Kap. C.II.3.).

Lösung Fall 3 (vgl. Empfehlung des EDÖB gemäss Art. 27 DSG betreffend Drogen- und Alkoholtests bei den Schweizerischen Bundesbahnen (SBB) in 15. TB, 2007/2008, 71 f.):
Zunächst fragt es sich, ob das DSG auf die vorliegende Fallgestaltung anwendbar ist, was davon abhängt, ob es sich um eine Datenbearbeitung durch ein Bundesorgan handelt (vgl. Art. 2 Abs. 1 DSG). Nach Art. 3 lit. h DSG gelten natürliche und juristische Personen, die mit öffentlichen Aufgaben des Bundes betraut sind, als Bundesorgane im Sinne des DSG. Obwohl die SBB (inzwischen) privatisiert sind, liegt diese Voraussetzung

vor, da sie mit öffentlichen Aufgaben des Bundes betraut sind, woran auch die privatrechtliche Organisationsform nichts ändert.
Eine Bearbeitung von Personendaten ist gegeben, da die Tests Angaben über die betroffenen Personen darstellen bzw. „produzieren" (nämlich über ihren Alkohol- und/oder Drogenkonsum).
Bei den von der SBB durchgeführten Drogen- und Alkoholtests handelt es sich um eine Datenbearbeitung von Gesundheitsdaten der Angestellten. Gesundheitsdaten beinhalten sämtliche Informationen, die direkt oder indirekt Rückschlüsse auf den physischen und psychischen Gesundheitszustand einer Person zulassen, die einen medizinischen Befund darstellen. Nach Art. 3 lit. c Ziff. 2 DSG gelten als besonders schützenswerte Personendaten u.a. Daten über die Gesundheit.
Um dem Grundsatz der Rechtmässigkeit Genüge zu tun, dürfen Bundesorgane besonders schützenswerte Personendaten nur bearbeiten, wenn dies ein Gesetz im formellen Sinne ausdrücklich erlaubt bzw. wenn ein entsprechender Ausnahmetatbestand vorliegt (Art. 17 DSG). Eine Rechtsgrundlage im formellen Sinne, d.h. in Form eines von der Bundesversammlung erlassenen Gesetzes, liegt jedoch im vorliegenden Fall nicht vor, da es sich bei der gesetzlichen Grundlage lediglich um Verordnungen bzw. Richtlinien handelt.
Bei Fehlen einer gesetzlichen Grundlage im formellen Sinn ist zu prüfen, ob allenfalls eine Ausnahme von Art. 17 Abs. 2 lit. a-c DSG greift. Dabei ist zu beachten, dass es sich bei den Aufzählungen in Art. 17 Abs. 2 lit. a-c DSG um Ausnahmebestimmungen handelt, die sich nur auf Aufgabenerfüllungen beziehen, die normalerweise keine Bearbeitung von Personendaten benötigen. Da jedoch anzunehmen ist, dass die Drogen- und Alkoholtests aus Sicherheitsgründen regelmässig vorgenommen werden, muss bereits aus diesem Grund das Greifen eines Ausnahmetatbestands verneint werden.
Damit erweist sich das Vorhaben der SBB als nicht mit den datenschutzrechtlichen Anforderungen in Einklang stehend, da dem Grundsatz der Rechtmässigkeit, im Zusammenhang mit dem Legalitätsprinzip, nicht entsprochen wird.

III. Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG)

Nach **Art. 4 Abs. 2 DSG** hat die Bearbeitung von Personendaten nach **Treu und Glauben** zu erfolgen.

Der Grundsatz von Treu und Glauben ist bereits in der **Bundesverfassung** in **Art. 5 Abs. 3 BV** sowie in **Art. 9 BV** verankert: Art. 5 Abs. 3 BV hält fest, dass sowohl staatliche Organe als auch Private nach Treu und Glauben zu handeln haben. Art. 9 BV statuiert, dass jede Person Anspruch darauf hat, von den staatlichen Organen ohne Willkür und nach Treu und Glauben behandelt zu werden. Dieser Grundsatz besagt allgemein, dass ein **loyales und vertrauenswürdiges Verhalten im Rechtsverkehr** grundlegend ist, dem widersprüchliches Verhalten zuwider läuft (Ehrenzeller/Mastronardi/Schweizer/ Vallender-HANGARTNER, Art. 5 BV, Rn. 43).
Durch die Einführung des Grundsatzes der Transparenz bzw. Erkennbarkeit sowie der Informationspflicht bei der Beschaffung besonders schützenswerter Daten und von Persönlichkeitsprofilen in Art. 4 Abs. 4, Art. 7a DSG (2. Kap. A.VI.) hat der Grundsatz von Treu und Glauben seine eigenständige Bedeutung für die von diesen Bestimmungen erfassten Verhaltensweisen verloren. Da diese jedoch nur das Beschaffen von Personendaten betreffen, behält der Grundsatz von Treu und Glauben seine Bedeutung für alle sonstigen **Formen der Bearbeitung von Personendaten nach dem Beschaffen**.

Der Grundsatz von Treu und Glauben ist insbesondere insofern von Bedeutung, als er eine **Generalklausel** darstellt und in all denjenigen Konstellationen zum Zuge kommt bzw. kommen kann, in denen die **anderen Bearbeitungsgrundsätze nicht greifen** (ROSENTHAL, Handkommentar, Art. 4 Rn. 14).

Angesichts des Umstandes, dass sich aus dem DSG keine allgemeine Pflicht ableiten lässt, Personen, deren Daten bearbeitet werden, in jedem Fall aktiv zu informieren, kommt dem Grundsatz von Treu und Glauben gerade in diesem Bereich eine wichtige Bedeutung zu: Ihm dürfte eine allgemeine Verpflichtung dergestalt zu entnehmen sein, dass die Betroffenen immer dann über die **Bearbeitung ihrer Daten zu informieren** sind, wenn sich dies angesichts der Umstände unter Zugrundelegung eines loyalen und vertrauenswürdigen Verhaltens aufdrängt.
So lässt sich aus diesem Grundsatz etwa eine Informationspflicht der betroffenen Personen über eine sie betreffende „Datenschutzpanne" (z.B. das unbeabsichtigte Aufschalten von Personendaten auf dem Internet oder eine sonstige versehentlich erfolgte Datenbekanntgabe an Dritte) ableiten.
Ebenso dürfte sich im Falle der grundsätzlich rechtmässigen Veröffentlichung von Personendaten auf dem Internet im Hinblick auf die Strafverfolgung (z.B. der Bilder einer Überwachungskamera zur Aufklärung einer Straftat) aus dem Grundsatz von Treu und Glauben eine grundsätzliche Pflicht ableiten lassen, mittels

eines vorherigen öffentlichen Aufrufs die Betroffenen aufzufordern, sich zu stellen, und im Falle des Unterlassens die Internetveröffentlichung anzukündigen.
Ebenfalls aus dem Grundsatz von Treu und Glauben ableitbar ist die grundsätzliche Pflicht der Datenbeschaffung direkt bei dem Betroffenen, nicht hingegen bei Dritten.

IV. Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG)

Fall 4:
Die SBB verlangen von ihren Angestellten, dass sie eine Erklärung auf Verzicht jeglichen (auch unregelmässigen oder punktuellen und in der Freizeit erfolgenden) Cannabiskonsums abgeben, dies im Hinblick auf die Erhöhung der Sicherheit und Qualität der Leistungen der SBB. Entspricht dieses Vorhaben dem Grundsatz der Verhältnismässigkeit?

Fall 5:
Der Eingang von zahlreichen Bundesämtern wird durch Videokameras überwacht, wobei Sicherheitsüberlegungen (Verhinderung bzw. Aufklärung von Einbrüchen oder auch Personenschäden) im Vordergrund stehen. Unter welchen Voraussetzungen steht eine solche Überwachung in Einklang mit dem Grundsatz der Verhältnismässigkeit?

Fall 6:
Der Direktor des Bundesamtes X hat den Eindruck, die Mitarbeiter und Mitarbeiterinnen seines Amtes nutzen das Internet – insbesondere die Kontaktseite „Facebook" – zu häufig zu privaten Zwecken. Er beschliesst daher, die Internetnutzung jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin zu speichern, dies im Hinblick auf eine entsprechende Kontrolle der Nutzung von Internetseiten durch jeden einzelnen Mitarbeiter oder jede einzelne Mitarbeiterin. Allerdings hegt er nach einem Gespräch mit dem Datenschutzberater des Departements (4. Kap. B.) Zweifel an der Verhältnismässigkeit dieser Massnahme. Zu Recht?

Art. 4 Abs. 2 DSG erwähnt neben dem Grundsatz von Treu und Glauben als Bearbeitungsgrundsatz auch den **Grundsatz der Verhältnismässigkeit**. Wie auch der Grundsatz von Treu und Glauben ist der Grundsatz der Verhältnismässigkeit bereits in der **Bundesverfassung** aufgeführt, so dass er jedenfalls durch die Bundesorgane zu beachten ist; eine Rechtfertigung seiner Nichtbeachtung ist nicht möglich.
Art. 5 Abs. 2 BV: „Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein."

Allgemein besagt der Grundsatz der Verhältnismässigkeit, dass eine staatliche Massnahme **geeignet und erforderlich** (also das mildeste Mittel) sein muss, um den mit dem öffentlichen Interesse verfolgten Zweck herbeizuführen und dass eine **Abwägung von öffentlichen Interessen und betroffenen privaten Interessen** (Verhältnismässigkeit i.e.S.) vorzunehmen ist.
Der Grundsatz der Verhältnismässigkeit ist insbesondere dann von besonderer Bedeutung, wenn eine gesetzliche Grundlage für die Datenbearbeitung sehr allgemein gehalten ist. Denn auch wenn eine solche Rechtsgrundlage einschlägig ist, darf eine Datenbearbeitung nicht ohne Einhaltung des Verhältnismässigkeitsprinzips vorgenommen werden. Mit anderen Worten ist die Geeignetheit, die Erforderlichkeit sowie die Verhältnismässigkeit i.e.S. (so dass die Datenbearbeitung auch unter Abwägung der in Frage stehenden Interessen zumutbar sein muss) einer Datenbearbeitung jeweils im Einzelnen zu hinterfragen und zu prüfen: Die Bearbeitungsgrundsätze müssen grundsätzlich in Bezug auf den Zweck sowie auf die Art der Bearbeitung erfüllt sein. Dies bedingt, dass Daten durch Bundesorgane von Vornherein nur dann bearbeitet werden dürfen, wenn sie für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich sind (BBl 1988 II 450).

Ob der Grundsatz der Verhältnismässigkeit eingehalten wird, kann nicht generell beantwortet werden, sondern ist **in jedem Einzelfall zu überprüfen**. Eine solche einzelfallabhängige Abklärung der Einhaltung der Anforderungen des Verhältnismässigkeitsgrundsatzes muss nach objektiven Kriterien vorgenommen werden, d.h. dass nicht auf die subjektive Sichtweise jeder einzelnen Person abzustellen ist (ROSENTHAL, Handkommentar DSG, Art. 4, Rn. 22 f.).

Jedenfalls impliziert die Heranziehung des Grundsatzes der Verhältnismässigkeit, dass in einem ersten Schritt der mit der entsprechenden **Datenbearbeitung verfolgte Zweck** eruiert wird, handelt es sich doch bei der Verhältnismässigkeit um eine **Mittel-Zweck-Relation**, so dass die Verhältnismässigkeit der herangezogenen Mittel nur in Bezug auf einen definierten Zweck (der natürlich rechtmässig sein muss, vgl. 2. Kap. A.II.) eruiert werden kann.

Für den Bereich des Datenschutzes können aus dem Verhältnismässigkeitsgrundsatz insbesondere folgende Vorgaben abgeleitet werden:

- Die Datenbearbeitung muss für die Erreichung des verfolgten Zwecks **geeignet** sein.

  Dies ist von Vornherein dann nicht der Fall, wenn eine Datensammlung lediglich „auf Vorrat" erfolgt, wobei hier auch schon der eigentliche Zweck der Datenbearbeitung nicht definiert ist (BGE 125 II 473 E. 4.b).

- Die Datenbearbeitung muss für die Erreichung des verfolgten Zwecks das **mildeste Mittel** darstellen und damit **erforderlich** sein, so dass Daten nur dann bearbeitet werden dürfen, wenn dies zur Erfüllung des Zwecks objektiv notwendig ist (vgl. auch BGE 125 II 473 E. 4).

- Schliesslich muss die Datenbearbeitung für den Betroffenen (wobei jede individuelle Person zu berücksichtigen ist) in Anbetracht des Zwecks und der verwandten Mittel zumutbar sein, so dass zwischen der Datenbearbeitung und dem damit verbundenen Eingriff in die Privatsphäre ein angemessenes Verhältnis bestehen muss (**Verhältnismässigkeit i.e.S.**).

Lösung Fall 4 (zur Frage des Vorliegens einer Datenbearbeitung sowie der Qualifikation der SBB als Bundesorgan siehe Lösung zu Fall 3):
Die Zielsetzung der Massnahme der SBB ist in der Erhöhung der Verkehrssicherheit und in der Verbesserung der Leistungen der SBB zu sehen. Diese Massnahme der SBB dürfte zwar zur Verfolgung dieser Zielsetzung geeignet sein, ist doch allgemein davon auszugehen, dass Personen, die nie (auch nicht in ihrer Freizeit) Cannabis konsumieren, grundsätzlich auch in der Arbeitszeit die Gewähr für Fahrtüchtigkeit und eine nicht durch Drogenkonsum beeinträchtigte Qualität der Arbeitsleistung bieten. Jedoch ist sie nicht erforderlich, denn es wird auch der Cannabis-Konsum in der Freizeit eruiert, der jedoch als solcher nicht notwendigerweise Auswirkungen auf die Arbeitsfähigkeit während der Arbeitszeit entfaltet. Damit handelt es sich um einen unverhältnismässigen Eingriff in die Privatsphäre und somit um einen Verstoss gegen den in Art. 4 Abs. 2 DSG niedergelegten Grundsatz der Verhältnismässigkeit.

Lösung Fall 5:
Von Bedeutung ist hier insbesondere die Frage der Erforderlichkeit. Aus diesem Grundsatz können folgende Anforderungen an eine derartige Videoüberwachung aus Sicherheitsüberlegungen formuliert werden:
- Gefilmt wird nur der zur Erfüllung des Sicherheitszweckes notwendige Radius.
- Die Aufnahmen werden nur so lange aufbewahrt, wie dies für den angestrebten Zweck notwendig ist. Dies impliziert, dass sie zu löschen sind, sobald feststeht, dass der Zweck erreicht ist. In der Regel wird hier (falls keine Straftaten begangen werden) eine Frist von 24 Stunden angemessen sein.
- Die Aufnahmen sind nur den mit der Überwachung der Sicherheit beauftragten Personen zugänglich; diese sind grundsätzlich zu nennen (vgl. zur rechtlichen Grundlage und dem Grundsatz der Rechtmässigkeit 2. Kap. A.II., 2. Kap. C.II.).

Zudem folgt aus dem Grundsatz der Transparenz bzw. der Erkennbarkeit (Art. 4 Abs. 4 DSG, unten 2. Kap. A.VI.), dass die Videoüberwachung für die Betroffenen (also diejenigen Personen, die sich im Aufnahmeradius befinden) erkennbar ist (etwa durch entsprechende Hinweisschilder oder durch ein klar sichtbares Anbringen der Kameras).

Lösung Fall 6:
Die fragliche Massnahme soll sicherstellen, dass die Mitarbeiter und Mitarbeiterinnen des betroffenen Bundesamtes ihre Arbeitszeit tatsächlich für ihre beruflichen Aufgaben einsetzen.
Die beschlossene Überwachungsmassnahme ist sicherlich ein geeignetes Mittel, diese Zielsetzung zu erreichen, denn sie ermöglicht eine Kontrolle der konsultierten Internetseiten und erlaubt damit grundsätzlich eine Antwort auf die Frage, inwieweit das Internet zu beruflichen oder privaten Zwecken genutzt wird.

Wird das Ziel der Massnahme so definiert, dass tatsächlich jeder „Missbrauch" des Internets am Arbeitsplatz zu privaten Zwecken unterbunden werden soll, so wäre die Massnahme möglicherweise sogar erforderlich: Will man nämlich wirklich jeden noch so unbedeutenden „Missbrauch" verhindern, dürfte eine „lückenlose" Überwachung der Internetnutzung jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin tatsächlich notwendig sein.
Hingegen bestehen grosse Zweifel an der Verhältnismässigkeit i.e.S. einer solchen Massnahme: Denn der massive Eingriff in die Persönlichkeitsrechte durch den Einblick in die „Internetgewohnheiten" jedes einzelnen Mitarbeiters dürfte in keinem vernünftigen Verhältnis zu dem „Gewinn" an Arbeitszeit stehen, zumal wenn man bedenkt, dass zahlreiche Mitarbeiter und Mitarbeiterinnen das Internet völlig korrekt nutzen dürften.
Vor diesem Hintergrund impliziert der Grundsatz der Verhältnismässigkeit i.e.S. ein „Zurückbuchstabieren" bei der Formulierung der Zielsetzung selbst, etwa in dem Sinn, dass lediglich übermässige Nutzungen des Internets für private Zwecke während der Arbeitszeit verhindert werden sollen. Dieses Ziel könnte dann durch eine „gruppenweise" Kontrolle der Internetnutzung (z.B. pro Abteilung) sichergestellt werden: Erst wenn sich aus dieser Kontrolle ergibt, dass in einer bestimmten Abteilung übermässig viel auf *a priori* nicht professionelle Seiten zurückgegriffen wird, können die einzelnen Arbeitsplätze überwacht werden (wobei die Betroffenen aber über diese Möglichkeiten in Kenntnis zu setzen sind, vgl. noch zum Grundsatz der Transparenz bzw. Erkennbarkeit unten 2. Kap. A.VI.). Falls es im Wesentlichen um die Nutzung bestimmter Internetseiten (wie z.B. „Facebook") geht, wäre eine andere, die Privatsphäre kaum beeinträchtigende Möglichkeit die Sperrung eben dieser Internetseite in dem betreffenden Amt.

V. Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG)

Fall 7 (hierzu SCHWEGLER, Datenschutz im Polizeiwesen, 91 f.):
Gemäss Art. 3 des DNA-Profil-Gesetzes (Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten und vermissten Personen, SR 363) dürfen sowohl von mutmasslichen Tätern schwerer Eigentumsdelikte oder von Opfern von Sexualdelikten DNA-Profile erstellt werden. In Anwendung dieser Bestimmung wurde von X als Opfer eines Sexualdelikts ein DNA-Profil erstellt. Zu einem späteren Zeitpunkt erhärtet sich der Verdacht, dass X in ein Eigentumsdelikt verwickelt sein könnte. Darf sein in Anwendung des Art. 3 DNA-Profil-Gesetzes erstelltes DNA-Profil mit den am Tatort des Eigentumsdelikts gefunden Täterspuren verglichen werden?

Nach **Art. 4 Abs. 3 DSG** dürfen Personendaten nur zu dem Zweck bearbeitet werden, der **bei der Beschaffung angegeben** wurde, aus den **Umständen ersichtlich** oder **gesetzlich vorgesehen** ist. Durch diesen so umschriebenen Grundsatz der Zweckbindung soll erreicht werden, dass den von einer Datenbearbeitung betroffenen Personen bereits zu Beginn deutlich wird, wofür ihre Daten verwendet werden und dass die Daten nicht „zweckentfremdet" werden.

Aus dieser Bestimmung lässt sich keine Pflicht entnehmen, dass Personen, deren Daten bearbeitet werden, in jedem Fall zu informieren wären. Eine Information der betroffenen Personen wird jedoch nicht ausgeschlossen und kann durch andere Bestimmungen vorzunehmen sein (etwa aufgrund des Grundsatzes von Treu und Glauben, Art. 4 Abs. 2 DSG, 2. Kap. A.III., oder aufgrund des Grundsatzes der Transparenz, Art. 4 Abs. 4 DSG, 2. Kap. A.VI., sowie bei der Beschaffung besonders schützenswerter Personendaten sowie von Persönlichkeitsprofilen, Art. 7a DSG.).

Für die Bundesverwaltung ist die Zweckbindung insbesondere im Zusammenhang mit einem bereits in einem **Gesetz vorgesehenen Zweck der Datenbearbeitung** von Bedeutung.

Denn Bundesorgane müssen sich bei der Bearbeitung von Personendaten grundsätzlich auf eine gesetzliche Grundlage stützen können (Art. 17 DSG), die bereits den Zweck der Datenbeschaffung festhält. Daher wird der Grundsatz der Zweckbindung bereits bei Einhaltung der für die jeweiligen Bundesorgane bereichsspezifischen Rechtsgrundlagen mitberücksichtigt, so dass der Zweck der Datenbeschaffung in den Fällen, in denen er bereits in der Rechtsgrundlage umschrieben wird bzw. sich aus dieser ergibt, bei der Datenbeschaffung nicht mehr explizit angegeben werden noch aus den Umständen ersichtlich sein muss.

Durch eine **neue gesetzliche Bestimmung** kann aber der ursprüngliche Zweck einer Datenbearbeitung modifiziert werden, so dass insofern eine gewisse Relativierung des Zweckbindungsgrundsatzes vorliegt. Die Zweckbindung ist hier (nur, aber immerhin)

insofern respektiert, als eine neue gesetzliche Grundlage besteht, die den „neuen“ Zweck umschreibt.

Gegen den Grundsatz der Zweckbindung verstösst etwa das Beschaffen von Personendaten „auf Vorrat“, da eine solche meist ohne konkretes Ziel und damit auch ohne Zweckbindung erfolgt (BGE 125 II 476 E. 4.b).
Ebenso darf der Personaldienst der Bundesverwaltung die Adressen von Bundesbeamten nur zum Zweck der Personalverwaltung (entsprechende Korrespondenz, Auszahlen von Löhnen usw.) verwenden, so dass es z.B. unzulässig (da mit dem Grundsatz der Zweckbindung unvereinbar) wäre, die Adressen von Angestellten mit einem bestimmten Einkommen an Verkaufsorganisationen zu vermitteln (BBl 1988 II 451).
Wird der Personalabteilung im Zusammenhang mit der Krankschreibung durch einen Angestellten ein Arztzeugnis eingereicht, dürfen die darin enthaltenen Personendaten nur dazu verwendet werden, die effektive Krankheit des Angestellten zu überprüfen, nicht hingegen zu anderen Zwecken.

Lösung Fall 7 (hierzu SCHWEGLER, Datenschutz im Polizeiwesen, 91 f.):
Ein solcher Abgleich ist nicht zulässig, so dass in einer dem Ausgangssachverhalt entsprechenden Fallgestaltung das DNA-Profil des Opfers eines Sexualdeliktes nicht mit den am Tatort des Eigentumsdelikts gefunden Täterspuren verglichen werden darf. Denn dies wäre mit dem Zweck des Opfer-DNA-Profils nicht vereinbar, da dieses lediglich die Abgrenzung zu den DNA-Profilen des Täters bzw. weiterer Beteiligter bezweckt (vgl. Art. 3 Abs. 1 lit. b DNA-Profil Gesetz).

VI. Grundsatz der Transparenz (Art. 4 Abs. 4 DSG)

Fall 8:
Die Abteilungsleiterin eines Bundesamtes hat den Eindruck, dass einer der Informatiker, mit dem seit längerem ein arbeitsrechtlicher Konflikt schwelt, ihren Mailverkehr einsieht. Sie beschliesst, die Nutzung des Computers durch den betreffenden Informatiker so kontrollieren zu lassen, dass sich dieser Verdacht erhärten oder entkräften lässt, was eine umfassende Einsicht in Mailverkehr und Internetnutzung durch den betreffenden Mitarbeiter impliziert. Da sie sich ihrer Sache nicht ganz sicher ist, beschliesst sie, den Mitarbeiter über diese Kontrollen nicht zu informieren. Steht dieses Vorhaben mit Art. 4 Abs. 4 DSG in Einklang?

Nach **Art. 4 Abs. 4 DSG** – der durch die am 1. Januar 2008 in Kraft getretene Revision (1. Kap. D.) in das DSG eingeführt wurde – muss die **Beschaffung von Personendaten**, insbesondere der Zweck ihrer Bearbeitung, für die betroffene Person **erkennbar** sein. Damit soll insbesondere eine transparente Datenbeschaffung für die betroffenen Personen sichergestellt werden (BBl 2003 2124).

Bemerkenswert ist, dass sich diese Erkennbarkeit nur auf die Beschaffung, nicht hingegen (wie bei den anderen Grundsätzen) auf die Bearbeitung als solche bezieht. Allerdings kann sich aus anderen Grundsätzen, insbesondere dem Grundsatz von Treu und Glauben, eine Informationspflicht der betroffenen Personen auch über die Bearbeitung ergeben (2. Kap. A.III.).

Unter welchen Voraussetzungen davon ausgegangen werden kann, dass die Beschaffung von Personendaten und der Bearbeitungszweck erkennbar sind, ist nach den **Umständen des Einzelfalls** zu entscheiden, wobei auch in diesem Zusammenhang der **Grundsatz von Treu und Glauben** eine Rolle spielt: So ist letztlich zu eruieren, von welchen Bearbeitungszwecken die Betroffenen in einem bestimmten Fall in guten Treuen ausgehen durften und zwar zu dem Zeitpunkt, zu dem die Beschaffung der Daten vorgenommen wurde (BBl 2003 2124 f.; ROSENTHAL, Handkommentar DSG, Art. 4, Rn. 34).

Werden z.B. die Daten direkt bei der betroffenen Person beschafft, ist dies für die Person ohne weiteres erkennbar und es müssen keine weiteren Schritte unternommen werden (BBl 1988 II 468). Es kann sich jedoch aufdrängen, dass eine betroffene Person über eine Datenbeschaffung informiert werden muss, ohne dass jedoch Art. 4 Abs. 4 DSG eine allgemeine Informationspflicht statuieren würde (Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des DSG, EDÖB, 10. Oktober 2007).

Bundesorgane dürfen Personendaten grundsätzlich nur aufgrund einer **gesetzlichen Grundlage** bearbeiten und somit beschaffen (2. Kap. A.II., C.II.). Bei einer Datenbeschaffung, sei dies direkt bei der betroffenen Person oder bei einer anderen Verwaltungsstelle, ist es daher ratsam, jeweils die rechtliche Grundlage der

Datenbeschaffung anzugeben, da somit nicht nur die Erkennbarkeit selbst gegeben ist, sondern auch über den Zweck der Datenbeschaffung informiert wird (JÖHRI, Handkommentar DSG, Art. 18, Rn. 28).
Werden bei einer **anderen Verwaltungsstelle** und somit einem **Dritten** Personendaten beschafft, stellt sich die Frage, inwiefern der Grundsatz der Erkennbarkeit gegenüber den betroffenen Personen erfüllt ist. Diese Frage ist jedenfalls dann zu bejahen, wenn sich aus der gesetzlichen Grundlage bereits die Weitergabemöglichkeit ergibt. Diese Konstellation ist schon deshalb die Regel, weil Bundesorgane Daten nur dann bearbeiten (und damit auch beschaffen) dürfen, wenn eine gesetzliche Grundlage vorhanden ist. Wenn die Beschaffung (ausnahmsweise) im Einzelfall in Anwendung des Art. 19 Abs. 1 lit. a DSG erfolgt (etwa auf Anfrage), so sind an die Erkennbarkeit grundsätzlich hohe Anforderungen zu stellen, da der Betroffene über diese Beschaffung grundsätzlich keine Kenntnis erhält und eine solche auch grundsätzlich nicht erwarten muss. Hier dürfte daher in aller Regel eine ausdrückliche Information notwendig sein.
Gemäss **Art. 7a DSG** besteht nunmehr seit dem 1. Januar 2008 bzw. dem 1. Januar 2009 (vgl. Übergangsbestimmung der Änderung vom 24. März 2006) eine aktive Pflicht zur Information beim **Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen,** nicht jedoch bei sämtlichen übrigen Personendaten, sofern eine Datensammlung angelegt wird. Diese Pflicht besteht auch, wenn solche Daten bei Dritten, so z.B. bei einer anderen Verwaltungsstelle, beschafft werden (Art. 7a Abs. 1 DSG). Art. 7a DSG geht damit weiter als der in Art. 4 Abs. 4 DSG enthaltene Grundsatz der Erkennbarkeit, wobei auch hier nur das Beschaffen, nicht sämtliches Bearbeiten von Personendaten betroffen ist. Für die **Bundesorgane** ist Art. 7a DSG insofern von Bedeutung, als grundsätzlich davon ausgegangen werden kann, dass bei einem Beschaffen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen gestützt auf eine gesetzliche Grundlage die Daten in eine Datensammlung aufgenommen werden.

Es besteht somit für Bundesorgane grundsätzlich beim Beschaffen solcher Daten eine Informationspflicht (JÖHRI, Handkommentar DSG, Art. 18, Rn. 16), es sei denn, die betroffene Person wurde bereits informiert (Art. 7a Abs. 4 DSG). Art. 7a Abs. 2 DSG führt diejenigen Informationen auf, die der betroffenen Person mindestens mitzuteilen sind, und Art. 7a Abs. 3 DSG präzisiert den Zeitpunkt, bis zu welchem der Informationspflicht spätestens nachzukommen ist. Ausnahmsweise kann die Informationspflicht entfallen (Art. 7a Abs. 4 DSG). Zu beachten sind in diesem Zusammenhang noch die Möglichkeiten einer Einschränkung der Informationspflicht, welche sich aus Art. 9 DSG ergeben (3. Kap. A.).

Zusammenfassend kann festgehalten werden, dass für die Einhaltung des Grundsatzes der Erkennbarkeit zunächst bei einer Datenbeschaffung abzuklären ist, ob es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile handelt. Wird dies bejaht, kommt Art. 7a DSG mit seiner Informationspflicht zur Anwendung, sofern die Daten in einer Datensammlung festgehalten werden. Wird dies hingegen verneint, sollte für die betroffene Person die Datenbeschaffung und deren Zweck zumindest erkennbar sein (Art. 4 Abs. 4 DSG). Hierbei ist grundsätzlich zu empfehlen, die gesetzliche Grundlage für die Datenbeschaffung anzugeben.

Die Kantone übermitteln gestützt auf das Strassenverkehrsgesetz (SVG, SR 741.01) beispielsweise Angaben über Führerausweisentzüge an das Bundesamt für Strassen zur Registrierung im Administrativmassnahmen-Register (vgl. Art. 104b SVG). Da die Kantone von ihnen beschaffte besonders schützenswerte Personendaten und Persönlichkeitsprofile im Rahmen des Vollzugs von Bundesrecht an Bundesbehörden weiterleiten, müssen sie auch die betroffenen Personen darüber informieren. Die Bundesbehörden trifft somit gestützt auf Art. 7a Abs. 4 lit. a DSG keine nochmalige Informationspflicht (BBl 2003 2133).

Ausnahmsweise kann aber das Beschaffen auch **ohne das Wissen der betroffenen Person** stattfinden, wenn hierfür eine **gesetzliche Grundlage** besteht. Dies ist insbesondere im Bereich der Polizei und der Strafverfolgung der Fall (JÖHRI, Handkommentar DSG, Art. 18, Rn. 31). Eine nachträgliche Information – die in der Regel dann greift, wenn der Zweck der Überwachungsmassnahmen durch eine Information nicht

mehr gefährdet wird – muss jedoch zwingend erfolgen (JÖHRI, Handkommentar DSG, Art. 18, Rn. 36).

Beispielsweise findet eine Überwachung des Post- und Fernmeldeverkehrs regelmässig ohne Wissen, d.h. ohne Erkennbarkeit für die betroffene Person statt (vgl. Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF, SR 780.1). So kann die Aufnahme eines Telefongesprächs geheim erfolgen. Dann muss aber, um dem Grundsatz der Erkennbarkeit Genüge zu tun, die betroffene Person im Nachhinein unter den erwähnten Voraussetzungen über die Datenbeschaffung informiert werden (JÖHRI, Handkommentar DSG, Art. 18, Rn. 11).

Lösung Fall 8:
Das Datenschutzgesetz findet auf die vorliegende Fallgestaltung Anwendung, denn es geht um ein Handeln eines Bundesorgans (das Verhalten der Abteilungsleiterin eines Bundesamtes ist als Verhalten eines Bundesamts anzusehen), und es steht die Beschaffung persönlicher Daten des betreffenden Mitarbeiters zur Debatte.
Eine solche Datenbeschaffung ist nur unter der Voraussetzung der Existenz einer gesetzlichen Grundlage zulässig (Art. 17 Abs. 1 DSG). Darüber hinaus muss die konkrete Art und Weise der Datenbeschaffung für den Betroffenen erkennbar sein (Art. 4 Abs. 4 DSG). Unabhängig von der Frage, ob in den einschlägigen rechtlichen Bestimmungen für eine solche Überwachung eine gesetzliche Grundlage besteht, stünde das Vorhaben nicht mit Art. 4 Abs. 4 DSG in Einklang: Denn für den betroffenen Mitarbeiter ist es nicht erkennbar, dass sein Mailverkehr und seine Internetnutzung einer solchen umfassenden individuellen Überwachung unterzogen wird. Daher könnte eine solche Überwachung – im Fall des Bestehens einer Rechtsgrundlage (die aber wohl kaum das Beschaffen solcher Daten ohne Information des betreffenden Mitarbeiters erlaubte) – nur unter der Voraussetzung der vorherigen Information des Betroffenen erfolgen.

VII. Grundsatz der Datenrichtigkeit und der Datensicherheit (Art. 5 Abs. 1, 7 DSG)

1. Datenrichtigkeit

Art. 5 Abs. 1 DSG – eine Vorschrift, die durch die am 1. Januar 2008 in Kraft getretene Revision um ihren zweiten Satz ergänzt wurde – enthält zwei voneinander zu trennende Pflichten der mit der Datenbearbeitung befassten Stelle:

- Wer Personendaten bearbeitet, hat sich nach **Art. 5 Abs. 1 S. 1 DSG** über deren **Richtigkeit zu vergewissern**.

  „Richtig" sind Personendaten immer dann, wenn sie eine Tatsache oder einen Umstand im Hinblick auf den Bearbeitungszweck **sachgerecht wiedergeben** (ROSENTHAL, Handkommentar, Art. 5, Rn. 1). Unrichtig in diesem Sinn können Personendaten damit auch dann sein, wenn sie an sich korrekte Angaben enthalten, jedoch im Hinblick auf den Bearbeitungszweck in irgendeiner Form irreführend sind (weil sie z.B. unvollständig sind oder die Information nicht in einen zutreffenden Gesamtzusammenhang stellen).
  Nach der Rechtsprechung des Bundesgerichts führen Einzelinformationen mit falschen Angaben nicht zwangsläufig zu unrichtigen Daten im Sinne des Art. 5 Abs. 1 S. 1 DSG, soweit und solange das wiedergegebene Gesamtbild zutreffend ist (BG 1A.6/2001, E. 2.c). Dieser Ansatz ist abzulehnen, denn Unrichtigkeit liegt jedenfalls dann vor, wenn **offensichtlich unrichtige Einzeltatsachen** vorliegen, unabhängig davon, ob sie das Gesamtbild verfälschen oder nicht (was mitunter auch streitig sein kann).
  Bei der Richtigkeit von Personendaten ist vor allem auch darauf zu achten, dass ein einmal richtiges Personendatum in der Zwischenzeit falsch werden kann (z.B. wenn bei einer Heirat eine Namensänderung erfolgt). Eine Ausnahme besteht dann, wenn es sich bei den aufgeführten Daten um eine **Momentaufnahme** handelt, bei welcher der Vergangenheitsbezug klar zum Ausdruck kommt und daher das bearbeitete Datum zwar aus heutiger Sicht als falsch gelten könnte, jedoch mit Blick auf den Sachzusammenhang mit der Vergangenheit durchaus als richtig verstanden wird (Maurer-Lambrou/Vogt-MAURER-LAMBROU, Art. 5, Rn. 7).
  Auch ein **Werturteil** kann „richtig" sein, wenn es im Hinblick auf den Bearbeitungszweck die Sachlage zutreffend wiedergibt. Ob ein Werturteil überhaupt bearbeitet werden darf, ist eine Frage der Verhältnismässigkeit (ROSENTHAL, Handkommentar DSG, Art. 5 Rn. 3). So kann die

Wiedergabe eines Verdachts durchaus eine „richtige" Information darstellen, z.B. wenn der Verdacht tatsächlich geäussert wurde oder für diesen Anhaltspunkte bestehen.

- Weiter hat der Datenbearbeiter nach **Art. 5 Abs. 1 S. 2 DSG** alle angemessenen Massnahmen zu treffen, damit im Hinblick auf den Bearbeitungszweck unrichtige oder unvollständige Daten ggf. **berichtigt oder vernichtet** werden. Obwohl dies in der etwas verunglückten Formulierung des Art. 5 Abs. 1 S. 2 DSG nicht eindeutig zum Ausdruck kommt, dürfte auch eine **Vernichtungspflicht** in den Fällen bestehen, in denen die Daten für den Bearbeitungszweck nicht mehr erforderlich sind. Diese Verpflichtung ergibt sich im Übrigen auch aus dem Verhältnismässigkeitsgrundsatz (2. Kap. A.IV.).

  Welche „angemessenen Massnahmen" zu ergreifen sind, hängt selbstredend von den Umständen des Einzelfalls ab. Jedenfalls besteht hier ggf. auch eine Pflicht, die sich nach den Umständen als sinnvoll und notwendig erweisenden **Kontrollmassnahmen** vorzusehen.
  Weiter müssen Personendaten grundsätzlich **nachgeführt und korrigiert** werden, es sei denn es handle sich lediglich um eine „Momentaufnahme".

2. Datensicherheit

a) Allgemeines

Nach dem in **Art. 7 DSG** verankerten **Grundsatz der Datensicherheit** müssen Personendaten durch **angemessene technische und organisatorische Massnahmen** gegen **unbefugtes Bearbeiten** geschützt werden.

Die Bedeutung der Datensicherheit kann kaum überschätzt werden: Denn ohne entsprechende Vorkehrungen kann das Anliegen des Datenschutzes völlig unterlaufen werden, da eine effektiver Schutz der Daten nicht erfolgt bzw. nicht erfolgen kann.

Dabei geht es in Art. 7 DSG allgemein um unbefugtes Bearbeiten von Daten, wobei drei Aspekte im Vordergrund stehen (vgl. auch Maurer-Lambrou/Vogt-PAULI, Art. 7, Rn. 2; ROSENTHAL, Handkommentar DSG, Art. 7, Rn. 7):

- **Vertraulichkeit**: Nur diejenigen Personen dürfen Zugriff auf die vorhandenen Daten haben, die auch über eine entsprechende Berechtigung hierfür verfügen.

- **Verfügbarkeit**: Die gewünschte Information hat in der gewünschten Form zum gewünschten Zeitpunkt am gewünschten Ort zur Verfügung zu stehen.

- **Datenintegrität**: Die Daten müssen richtig sein (2. Kap. A.VII.1.). Dies bedingt jedoch, dass durch die Bearbeitungsvorgänge keine unzulässigen Änderungen der Daten vorgenommen werden. Dies kann z.B. aufgrund eines Computervirus oder eines Datenübertragungsfehlers der Fall sein.

Darüber hinaus ist aber auch **jegliche sonstige unbefugte Bearbeitung** der Daten zu verhindern, etwa durch eine unverhältnismässige oder zweckwidrige Datenbearbeitung.
Welche Massnahmen „angemessen" im Sinne des Art. 7 DSG sind, ist nach den **Umständen des Einzelfalls** zu entscheiden, wobei allgemein festzuhalten ist, dass die Massnahmen dem Verhältnismässigkeitsgrundsatz entsprechen müssen und die Anforderungen an die zu ergreifenden Massnahmen mit dem Gefährdungspotential bzw. der Schwere des Eingriffs in die Privatsphäre ansteigen.

Art. 8 Abs. 2 VDSG (auf den der für Bundesorgane massgebliche Art. 20 Abs. 1 VDSG verweist) nennt in einer nicht abschliessenden Liste die bei der Wahl der angemessenen Massnahmen jedenfalls zu beachtenden **Kriterien**: Zweck der Datenbearbeitung, Art und Umfang der Datenbearbeitung, Einschätzung der möglichen Risiken für die betroffenen Personen, Stand der Technik. Zudem sind die Massnahmen „periodisch" zu überprüfen (Art. 8 Abs. 3 VDSG), wobei die Periodizität auch von den Umständen des

Einzelfalls abhängen dürfte; die Zeitspannen dürfen aber keinesfalls zu lang gewählt sein, und im Falle geänderter Umstände muss ggf. auch sofort eine Überprüfung erfolgen.

Als Massnahmen kommen **technische und organisatorische Massnahmen** in Betracht (vgl. zu den einzelnen Massnahmen auch den vom EDÖB herausgegebene „Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes“, 1994):

- **Technische Massnahmen**: Dazu sind die klassischen IT-Sicherheitsmassnahmen zu zählen, insbesondere die Einführung eines Passwortes oder die Datenverschlüsselung (vgl. Anhang 1 WIsB). Hierunter können aber auch **bauliche Massnahmen** fallen: Diese beinhalten z.B. die Sicherung von Daten in einem abschliessbaren Raum, zu dem nur berechtigte Personen Zutritt haben.

- **Organisatorische Massnahmen**: Hierzu gehören z.B. die Instruierung der Benutzer (z.B. in Bezug auf den Umgang mit Passwörtern) sowie die Dokumentation beispielsweise einer technischen Massnahme.

Art. 20 ff. VDSG (i.V.m. Art. 8-10 VDSG) enthalten noch einige Präzisierungen der zu ergreifenden Massnahmen, wobei insbesondere auf folgende Aspekte hinzuweisen ist:

- Die Systeme der Datenbearbeitung müssen insbesondere vor unbefugter oder zufälliger Vernichtung, zufälligem Verlust, technischen Fehlern, Fälschung, Diebstahl oder widerrechtlicher Verwendung, unbefugtem Ändern, Kopieren, Zugreifen oder **anderer unbefugter Bearbeitung geschützt** werden (Art. 8 Abs. 1 lit. a-e i.V.m. Art. 20 Abs. 1 VDSG).

- Art. 9 i.V.m. Art. 20 VDSG führt die **Ziele** auf, die durch die technischen und organisatorischen Massnahmen bei der **automatisierten Bearbeitung von Personendaten** erreicht werden sollen (z.B. Zugangskontrolle, Bekanntgabekontrolle, Zugriffskontrolle).

- Bei einer **automatisierten Bearbeitung von besonders schützenwerten Personendaten oder Persönlichkeitsprofilen** hat eine **Protokollierung** stattzufinden, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können (Art. 10 i.V.m. Art. 20 Abs. 1 VDSG).

- Für **automatisierte Datensammlungen**, die besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten, durch mehrere Bundesorgane benutzt werden, Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht werden oder mit anderen Datensammlungen verknüpft sind, hat das verantwortliche Bundesorgan ein **Bearbeitungsreglement** zu erstellen (Art. 21 Abs. 1 VDSG). Art. 21 Abs. 2 VDSG enthält Vorgaben über die in einem solchen Reglement zu berücksichtigenden Aspekte.

Insgesamt spricht Vieles dafür, dass es die Vorgaben in Art. 7 Abs. 1 DSG und Art. 8 ff., 20 ff. VDSG – wobei letztere recht detailliert ausfallen – grundsätzlich verlangen, dass die Datenbearbeiter verpflichtet werden, ein **umfassendes Sicherheitskonzept** zu erarbeiten, in dessen Rahmen alle Aspekte der Datensicherheit Berücksichtigung finden müssen. Z.B. müssen technische Massnahmen durch entsprechende organisatorische Massnahmen ergänzt werden, damit erstere nicht ineffektiv werden (etwa durch die Weitergabe von Passwörtern o.ä.). Im Rahmen eines solchen Konzepts sind im Einzelnen die bearbeiteten Daten und das Gefährdungspotential zu eruieren, um sodann – in Anwendung der skizzierten gesetzlichen Vorgaben – die zu erreichenden Ziele zu formulieren, die ihrerseits Grundlage für die zu ergreifenden „angemessenen Massnahmen“ bilden.
Nach **Art. 22 Abs. 2 VDSG** bleibt ein **Bundesorgan** auch dann weiterhin für den Datenschutz verantwortlich, wenn es **Personendaten durch Dritte** bearbeiten lässt (vgl. auch 2. Kap. C.I.).

b) Insbesondere: zur Informatiksicherheit in der Bundesverwaltung

Es liegt auf der Hand, dass die Informatiksicherheit für die Effektivität des Datenschutzes eine zentrale Rolle spielt, so dass im Folgenden ein Überblick über die Sicherstellung der Informatiksicherheit in der Bundesverwaltung gegeben werden soll.
In der Bundesverwaltung übernimmt das **Informatikstrategieorgan Bund (ISB)** als Stabstelle des **Informatikrates Bund (IRB)** die Erarbeitung der Entscheidungsgrundlagen für die strategische Steuerung der Informatik in der Bundesverwaltung (vgl. auch www.isb.admin.ch). Der IRB seinerseits trägt die Gesamtverantwortung für die **Informations- und Kommunikationstechniken (IKT)** in der Bundesverwaltung.

Die Elemente der Verfügbarkeit, der Vertraulichkeit, der Integrität sowie der Nachvollziehbarkeit von Informationen und Daten bilden zusammen mit der IKT-Strategie Bund, der Bundesinformatikverordnung und der Informationsschutzverordnung die Grundlagen für die Sicherheitsvorgaben in der Bundesverwaltung:

- **IKT-Strategie Bund**: Diese Strategie, die für die Jahre 2007-2011 definiert wurde, zeigt auf, wie sich der Einsatz der Informations- und Kommunikationstechnik in der Bundesverwaltung bis 2011 entwickeln soll.

  Die **IKT Strategie 2007** kann unter http://www.isb.admin.ch → Themen → Strategien eingesehen werden.

- **Bundesinformatikverordnung** (Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung, BinfV, SR 172.010.58): Sie regelt die Aufgaben und Zuständigkeiten bei der Planung und dem Einsatz der Informations- und Kommunikationstechnik in der Bundesverwaltung.

- **Informationsschutzverordnung** (Verordnung über den Schutz von Informationen des Bundes, ISchV, SR 510.411): Regelungsgegenstand ist der Schutz von Informationen des Bundes und der Armee (Art. 1).

Als eine der wichtigsten Vorgaben für die Datensicherheit in der Informatik sind die **Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004** (WIsB) zu sehen. Die Weisungen regeln für den Bereich der Informatiksicherheit in der Bundesverwaltung die Organisation, das Sicherheitsverfahren sowie die Netzwerksicherheit (Art. 1 Abs. 1). Zudem bestimmen sie die technischen, baulichen, organisatorischen und personellen Anforderungen und Massnahmen (Art. 1 Abs. 2). Anhang I der Weisungen sind die minimalen Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf zu entnehmen, wohingegen Anhang 2 die Definitionen und Sicherheitsvorgaben für die Netzwerksicherheit enthält.

B Datenübermittlung ins Ausland

Literatur: Maurer-Lambrou/Vogt-STEINER, Art. 6 DSG; SCHWAB, SJZ 2004, 125 ff.; WALTER, in: Epiney/Hobi, La révision de la Loi sur la protection des données, 99 ff.; EDÖB, Dritter Tätigkeitsbericht; EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz; EDÖB, Erläuterung zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG; EDÖB, Die Datenübermittlung ins Ausland kurz erklärt.

Fall 9:
Das Bundesamt für Migration hat das Asylgesuch von X nach den einschlägigen Vorgaben im Asylgesetz entgegengenommen und in diesem Zusammenhang auch eine Reihe von Daten über X bearbeitet (u.a., neben den Personalien, Angaben über Aufenthaltsorte und Reisewege sowie die Motivation des Asylgesuchs). Der Staat I – der nicht auf der nach Art. 7 VSDG erstellten Liste des EDÖB figuriert – gelangt mit der Anfrage an das Bundesamt heran, ihm alle über X verfügbaren Daten zu übermitteln: X sei ein Terrorist und werde wegen der Vorbereitung und Durchführung terroristischer Anschläge in I polizeilich gesucht. Könnte die Übermittlung dieser Daten zulässig sein?

Obwohl die **Datenbearbeitung über die nationalen Grenzen** hinaus heute in fast allen Bereichen der staatlichen Tätigkeit etwas Alltägliches ist, bleibt der grenzüberschreitende Datenverkehr t im Vergleich zu einer rein „nationalen" Datenbearbeitung mit zusätzlichen **Gefahren für die Persönlichkeitsrechte** Betroffener verbunden.

Zunächst ist bei einem Datentransfer ins Ausland die Gefahr, dass diese für die Betroffenen nicht erkennbar ist, häufig grösser. Auch stösst die Durchsetzung der Rechte der Betroffenen (3. Kap.) sowie die Ausübung der Kontrollrechte (4. Kap. A.) auf zusätzliche Schwierigkeiten, so dass ihre Effektivität häufig beeinträchtigt ist. Schliesslich – und vor allem – ist dem Umstand Rechnung zu tragen, dass zahlreiche Staaten ein tieferes Datenschutzniveau als die Schweiz aufweisen, so dass mit einer Datenübermittlung ins Ausland die Gefahr einher geht, dass dort mit diesen Daten Bearbeitungen durchgeführt werden, die in der Schweiz nicht erlaubt wären.

Vor diesem Hintergrund formuliert **Art. 6 DSG spezifische Vorgaben an die grenzüberschreitende Bekanntgabe von Personendaten** ins Ausland. Diese stellen für eine bestimmte Art der Datenbearbeitung – nämlich die grenzüberschreitende Bekanntgabe – besondere Rechtmässigkeitsvoraussetzungen auf, die letztlich die allgemeinen Grundsätze (2. Kap. A.) für diesen Bereich spezifizieren. Es ist aber nachdrücklich darauf hinzuweisen, dass über die in Art. 6 DSG enthaltenen Anforderungen hinaus immer auch die erörterten **allgemeinen datenschutzrechtlichen Prinzipien** – wobei den Grundsätzen der Verhältnismässigkeit und der Zweckbindung sowie (für Bundesorgane) dem Erfordernis einer gesetzlichen Grundlage (2. Kap. C.II.) eine besondere Bedeutung zukommen dürfte – zu beachten sind. Insofern ist es also denkbar, dass bei einer (geplanten) grenzüberschreitenden Bekanntgabe von Daten zwar die Voraussetzungen des Art. 6 DSG eingehalten worden sind, diese aber wegen Verstosses gegen einen der in Art. 4 DSG genannten Grundsätze gleichwohl zu unterbleiben hat.

Art. 6 DSG wurde im Zuge der am 1.1.2008 in Kraft getretenen Revision des DSG modifiziert, wobei insbesondere von Bedeutung ist, dass neu Anforderungen der Datenübermittlung ins Ausland für diejenigen Fälle, in denen die dort einschlägige Gesetzgebung keinen ausreichenden Schutz gewährleistet, definiert, womit nunmehr auch im Falle fehlenden gleichwertigen Schutzes eine Datenübermittlung ins Ausland unter den noch aufzuzeigenden Voraussetzungen möglich ist.

Im Einzelnen formuliert Art. 6 DSG einerseits einen **Grundsatz** (I.), andererseits **Ausnahmen von diesem Grundsatz** (II.).

Falls Personendaten der Öffentlichkeit über einen automatisierten Informations- und Kommunikationsdienst zugänglich gemacht werden, z.B. im **Internet,** stellt dies keine Übermittlung ins Ausland dar (Art. 5 VDSG). Damit geht die Verordnung letztlich von demselben Ansatz aus wie der EuGH in der Rs. *Lindqvist* (1. Kap. B.II.2.).

Eine grenzüberschreitende Bekanntgabe im Sinne des Art. 6 DSG liegt auch nicht vor, wenn lediglich Daten (etwa in Akten oder in einem Notebook) ins Ausland mitgeführt werden, dort jedoch niemandem zugänglich gemacht werden.

I. Grundsatz (Art. 6 Abs. 1 DSG)

Angesichts der erwähnten Gefahren für die Persönlichkeitsrechte der Betroffenen, die mit einer grenzüberschreitenden Bekanntgabe von Persönlichkeitsdaten grundsätzlich verbunden sind oder zumindest sein können, formuliert Art. 6 Abs. 1 DSG den Grundsatz, dass die **Bekanntgabe von Personendaten ins Ausland untersagt** ist, wenn dadurch die „Persönlichkeit" (gemeint sind wohl die Persönlichkeitsrechte) der betroffenen Person **schwerwiegend gefährdet** wird.

Bemerkenswert ist hier, dass bereits aufgrund des Wortlauts des Art. 6 Abs. 1 DSG eine schwerwiegende **Gefährdung** der Persönlichkeitsrechte des Betroffenen ausreichend ist, so dass also diesbezüglich keine Sicherheit verlangt werden darf, sondern bereits die Gefahr einer solchen Beeinträchtigung zur grundsätzlichen Unzulässigkeit der Datenübermittlung ins Ausland führt.

Eine solche schwerwiegende Gefährdung ist gemäss Art. 6 Abs. 1 DSG namentlich dann anzunehmen, wenn eine **Gesetzgebung** fehlt, die einen **angemessenen Schutz** gewährleistet, so dass bei Vorliegen dieser Voraussetzung **von Gesetzes wegen** von einer schwerwiegenden Gefährdung der Persönlichkeit auszugehen ist. Es ist aber zu betonen, dass diese Konstellation nur einen Anwendungsfall darstellt, bei dem eine schwerwiegende Gefährdung der Persönlichkeitsrechte (zwingend) anzunehmen ist. Bereits der Wortlaut des Art. 6 Abs. 1 DSG lässt aber erkennen, dass auch **andere Fallgestaltungen** denkbar sind, in denen eine solche schwerwiegende Gefährdung zu bejahen sein kann.

So dürfte etwa regelmässig auch dann eine schwere Verletzung der Persönlichkeitsrechte zu gewärtigen sein, wenn Personendaten an einen Staat bekannt gegeben werden sollen, der die Menschenrechte nicht respektiert, oder der Empfänger eine kriminelle Organisation im Ausland ist. Ebenso ist die Lage zu beurteilen, wenn in einem Staat zwar eine „angemessene" Datenschutzgesetzgebung besteht, diese jedoch nicht angewandt wird, so dass bei der Frage, ob und inwieweit die Gesetzgebung des in Frage stehenden Staates einen angemessenen Schutz gewährleistet, eben auch auf die Umsetzung in der Praxis abzustellen ist.
Der EDÖB führt eine **Liste** mit Staaten, die seiner Ansicht nach einen angemessenen Schutz gewährleisten (Art. 7 VDSG). Staaten, die das **Übereinkommen des Europarats vom 28. Januar 1981** (1. Kap. B.I.3.b) zum Schutze des Menschen bei einer automatischen Verarbeitung personenbezogener Daten ratifiziert haben, gewährleisten in der Regel einen gleichwertigen Schutz.

Deutlich wird damit, dass der zu erwartende Schutz der Persönlichkeitsrechte der betroffenen Person jedenfalls von **Fall zu Fall** und für **jede einzelne Bekanntgabe** zu prüfen ist; dies gilt nach dem Gesagten auch für die Bekanntgabe in Staaten, in denen aufgrund der einschlägigen Gesetzgebung grundsätzlich ein angemessener Schutz gewährleistet ist. Bei dieser Einzelfallprüfung sind die Umstände der Bekanntgabe zu berücksichtigen, insbesondere die Art der Daten, der Zweck der Bearbeitung, die in dem betreffenden Staat einschlägigen Rechtsvorschriften sowie der Empfänger der Daten bzw. die Zugangsberechtigten.

II. Ausnahmen (Art. 6 Abs. 2 DSG)

Ausnahmsweise – Art. 6 Abs. 2 DSG dürfte als Ausnahmevorschrift vom Grundsatz des Art. 6 Abs. 1 DSG grundsätzlich eng auszulegen sein – können in den Fällen, in denen die **Gesetzgebung des betreffenden Staates keinen angemessenen Schutz** gewährleistet, Personendaten gleichwohl ins Ausland bekannt gegeben werden. Diese Fälle zählt das Gesetz **abschliessend** in **Art. 6 Abs. 2 DSG** auf. Die Daten können demnach, trotz fehlendem gesetzlichem Schutz, bekannt gegeben werden, wenn

- **hinreichende (vertragliche) Garantien** bestehen (Art. 6 Abs. 2 lit. a DSG);

- die betroffene Person in die Bekanntgabe **eingewilligt** hat (Art. 6 Abs. 2 lit. b DSG);
- die Datenbearbeitung in unmittelbarem Zusammenhang mit **Abschluss oder Abwicklung eines Vertrages** steht und es sich um Personendaten des Vertragspartners handelt (Art. 6 Abs. 2 lit. c DSG);
- die Bekanntgabe im Einzelfall für die **Wahrung eines überwiegenden öffentlichen Interesses** oder für die Feststellung, Ausübung und Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist (Art. 6 Abs. 2 lit. d DSG);

  Der Ausnahmetatbestand der Wahrung eines **überwiegenden öffentlichen Interesses** dürfte für die Bundesverwaltung von besonderer Bedeutung sein. Seine rechtliche Tragweite kann durch folgende Aspekte präzisiert werden:
  - Die Bekanntgabe ist nur im **Einzelfall** zulässig, also nicht in systematischer Weise.
  - Die Frage, ob ein überwiegendes öffentliches Interesse vorliegt, ist aus der **Perspektive der Schweiz** bzw. der schweizerischen Rechtsordnung zu beurteilen. Allerdings kann darunter auch ein **öffentliches Interesse eines anderen Staates** (z.B. an der Aufrechterhaltung der inneren Sicherheit) fallen.
  - Die Bekanntgabe ist tatsächlich **unerlässlich**, so dass ihre Unterlassung die Verwirklichung des angestrebten öffentlichen Interesses verunmöglichte.
  - Das öffentliche Interesse muss **„überwiegend"** sein, dies im Verhältnis zu der mit der Bekanntgabe einhergehenden Persönlichkeitsverletzung. Ob dies der Fall ist, ist anhand aller Umstände des Einzelfalls zu beurteilen, wobei auch die vom Empfängerstaat gegebenen Garantien zu berücksichtigen sind.

  In zahlreichen Fällen enthält die schweizerische Gesetzgebung **spezifische Vorgaben**, die die grenzüberschreitende Bekanntgabe von Daten unter bestimmten Voraussetzungen und in bestimmten Konstellationen erlauben. In diesen Fällen kommt Art. 6 DSG nur eine marginale Bedeutung zu; allerdings sind seine Voraussetzungen ggf. jeweils zusätzlich zu beachten, so dass insbesondere das Interesse der Betroffenen gebührend zu berücksichtigen ist.
- die Bekanntgabe im Einzelfall erforderlich ist, um das **Leben oder die körperliche Integrität der betroffenen Person** zu schützen (Art. 6 Abs. 2 lit. e DSG);
- die betroffene Person die **Daten allgemein zugänglich** gemacht hat und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 6 Abs. 2 lit. f DSG) oder
- die Bekanntgabe **innerhalb derselben Firma oder desselben Konzerns** stattfindet, sofern innerhalb dieser Firma oder dieses Konzerns Datenschutzregeln gelten, die einen angemessen Schutz gewährleisten (Art. 6 Abs. 2 lit. g DSG).

Nach **Art. 6 Abs. 3 DSG** ist der **EDÖB** über gewisse Aspekte der Anwendung der **Ausnahmebestimmungen zu informieren** (nämlich in den Fällen des **Art. 6 Abs. 2 lit. a und g DSG**); es handelt sich hier nur um eine Meldepflicht, nicht um eine Genehmigungspflicht. Immerhin hat die Meldung nach Art. 6 Abs. 1 VDSG grundsätzlich im Vorfeld der Bekanntgabe ins Ausland zu erfolgen; eine Ausnahme gilt nur für die Fälle, in denen eine vorgängige Information „nicht möglich" ist, eine Konstellation, die zumindest im Rahmen der Bundesverwaltung allenfalls ausnahmsweise zu bejahen sein dürfte. Art. 6 Abs. 2, 3 VDSG sind darüber hinaus Einzelheiten über diejenigen Konstellationen zu entnehmen, bei denen von der Erfüllung der Informationspflicht auszugehen ist. Der EDÖB hat die ihm mitgeteilten Garantien und Datenschutzregeln zu **prüfen** und dem Inhaber der Datensammlung innerhalb von 30 Tagen das Ergebnis seiner Prüfung mitzuteilen (Art. 6 Abs. 5 VDSG). Die Meldepflicht befreit den Inhaber einer Datensammlung nicht von seiner Verantwortung: Er muss die materiellen Regeln des Gesetzes einhalten. Gleich wie bei einer nicht meldepflichtigen Datensammlung bzw. Übermittlung muss er das Risiko einer Persönlichkeitsverletzung selber beurteilen.

Art. 328b OR – Schutz der Persönlichkeit des Arbeitnehmers bei der Bearbeitung von Personendaten – geht den allgemeinen Bestimmungen des DSG vor. Datenbekanntgaben an Behörden im Rahmen gesetzlicher Pflichten des Arbeitgebers gehören zu denjenigen, die zur Durchführung des Arbeitsvertrags erforderlich

sind. Wenn eine gesetzliche Pflicht zur Datenbekanntgabe besteht, ist eine dazu erforderliche Übermittlung nicht meldepflichtig im Sinne von Art. 6 Abs. 2 DSG (vgl. VPB 59.31).

Wortlaut und Sinn und Zweck des Art. 6 Abs. 2 DSG in Verbindung mit dem Grundsatz des Art. 6 Abs. 1 DSG legen die Annahme nahe, dass Abweichungen nach Art. 6 Abs. 2 DSG nur in denjenigen Fallkonstellationen erfolgen dürfen, in denen die **Gesetzgebung in dem betreffenden Staat keinen ausreichenden Schutz** gewährleisten. Im Umkehrschluss wird man daraus schliessen können, dass nicht nur in jedem Fall einer „ungenügenden" Gesetzgebung der Datentransfer untersagt ist (es sei denn, eine der Ausnahmen des Art. 6 Abs. 2 DSG sei einschlägig), sondern auch, dass der Grundsatz des Art. 6 Abs. 1 DSG, wonach im Falle der Gefahr schwerwiegender Persönlichkeitsrechtsverletzungen von einer Datenübermittlung abzusehen ist, ansonsten nicht durchbrochen werden darf.

Lösung Fall 9:
Das Bundesamt für Migration ist ein Bundesorgan und darf daher Daten nur unter der Voraussetzung des Bestehens einer gesetzlichen Grundlage bearbeiten (Art. 17 Abs. 1 DSG). Diese kann nicht in Art. 98 AsylG gesehen werden, da diese Bestimmung nur die Bekanntgabe von Daten erlaubt, wenn dies dem Vollzug des Asylgesetzes dient. Im vorliegenden Fall geht es aber um eine strafrechtliche Verfolgung. Allerdings kann grundsätzlich Art. 19 Abs. 1 lit. a DSG einschlägig sein, der eine Bekanntgabe erlaubt, wenn die Daten für den Empfänger im Einzelfall zu Erfüllung seiner gesetzlichen Aufgaben unentbehrlich sind. Diese Bestimmung erlaubt auch die Datenbekanntgabe ins Ausland und grundsätzlich könnten die Voraussetzungen dieser Vorschrift im Ausgangsfall gegeben sein.
Allerdings sind jedenfalls die Voraussetzungen des Art. 6 DSG zu beachten. Da der Staat I nicht auf der Liste des EDÖB figuriert, ist davon auszugehen, dass er nicht über eine Gesetzgebung verfügt, die einen angemessenen Schutz gewährleistet. Daher ist eine Bekanntgabe nur unter den Voraussetzungen des Art. 6 Abs. 2 DSG zulässig. Einschlägig sein könnte hier Art. 6 Abs. 2 lit. d DSG, da es bei der strafrechtlichen Verfolgung von „Terroristen" um ein überwiegendes öffentliches Interesse gehen könnte. Ein solches könnte im Ausgangsfall grundsätzlich vorliegen, auch wenn es nicht zwingend um die innere Sicherheit in der Schweiz geht, da auch aus schweizerischer Sicht die Bekämpfung terroristischer Aktivitäten zweifellos ein öffentliches Interesse darstellt. Allerdings sind bei der vorzunehmenden Interessenabwägung die genauen Umstände des Einzelfalls zu beachten, dies im Hinblick auf die Eruierung des Vorliegens der Voraussetzungen des Art. 6 Abs. 2 lit. d DSG. Von Bedeutung dürften etwa folgende Elemente sein:

- Respektiert der Staat I allgemein seine menschenrechtlichen Verpflichtungen nicht und sind z.B. Folter oder „Sippenhaftung" durch staatliche oder staatlich kontrollierte Organe verbreitet, dürfte eine Bekanntgabe unzulässig sein, da die Rechte des Betroffenen zu weitgehend eingeschränkt werden und im Übrigen Art. 6 Abs. 2 in einem solchen Fall keine Ausnahme erlauben dürfte.
- Der Staat I müsste glaubhafte Garantien abgeben, dass die Daten tatsächlich für den angegebenen Zweck verwendet werden.
- Die Datensicherheit müsste sichergestellt werden.

Über die Vorgaben des Art. 6 DSG hinaus sind aber auch die allgemeinen datenschutzrechtlichen Grundsätze zu beachten. Von Bedeutung könnte in unserem Zusammenhang insbesondere der Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG) sein: Die Daten des X wurden zum Zweck der Erledigung seines Asylantrags bearbeitet. Hier hingegen geht es um deren Verwendung zur Strafverfolgung, was einen anderen Zweck darstellt, so dass die Übermittlung zumindest aus diesem Grund unzulässig sein dürfte.

C Spezifische Vorgaben für Bundesorgane

Literatur: Maurer-Lambrou/Vogt-JÖHRI/STUDER, Art. 16-21 DSG; Maurer-Lambrou/Vogt-WINTERBERG-YANG, Art. 22 DSG; Maurer-Lambrou/Vogt-KUNZ, Art. 23 DSG; Maurer-Lambrou/Vogt-BANGER, Art. 23 DSG; SCHEFER, in: Epiney/Hobi, Revision des Datenschutzgesetzes, 67 ff.; EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetz über den Datenschutz; EDÖB-Newsletter „datum"; EDÖB, Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung; Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, SR 88.032; 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 der Menschen bei der automatischen Verarbeitung von Personendaten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung vom 19. Februar 2003, SR 03.016; EDÖB, Kommentar zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11).

Das DSG gilt sowohl für die Bearbeitung von Personendaten durch Private als auch durch Bundesorgane (Art. 2 Abs. 1 DSG, 1. Kap. D.). Gleichwohl enthält es aber auch **spezifische Vorgaben bzw. Regelungen für Bundesorgane**, die im Übrigen in Ausübung ihrer hoheitlichen Tätigkeiten oder auch privatrechtlich handeln können. Vor diesem Hintergrund können die für Bundesorgane geltenden materiell-rechtlichen Vorgaben des Datenschutzgesetzes (daneben sind selbstredend immer auch die spezialgesetzlichen Vorgaben zu beachten) wie folgt zusammengefasst werden:

- Jedenfalls zur Anwendung kommen die im zweiten Abschnitt des DSG (Art. 4 ff. DSG) enthaltenen **allgemeinen Datenschutzbestimmungen**, wobei ihre konkrete Bedeutung für die Bundesorgane aber durchaus variiert.

- Spezifische Vorgaben für Bundesorgane, die diese immer dann zu beachten haben, wenn sie in Ausübung ihrer gesetzlichen bzw. hoheitlichen Aufgaben handeln, enthält der vierte Abschnitt des DSG (Art. 16 ff. DSG).

  Diese Bestimmungen sind – da der Staat hier den Einzelnen als Träger von Hoheitsgewalt gegenübertritt – in manchen Punkten strenger ausgestaltet als die für die Datenbearbeitung durch Private (dritter Abschnitt des DSG, Art. 12 ff. DSG) geltenden Regelungen.

- Handeln **Bundesorgane** hingegen **privatrechtlich**, so dass nicht öffentliches Recht, sondern Privatrecht auf das Rechtsverhältnis Anwendung findet, gelten die für **Private anwendbaren Bestimmungen auch für Bundesorgane** (Art. 23 DSG), wobei sich die Aufsicht aber auch hier nach Art. 27 DSG richtet (4. Kap. A.).

  Im Zusammenhang mit Art. 23 DSG ist es damit wichtig abzuklären, wann ein Bundesorgan hoheitlich und wann privatrechtlich handelt. Ist diese Frage geklärt, kommen entweder die privatrechtlichen oder öffentlich-rechtlichen Bestimmungen des DSG zur Anwendung. Bundesorgane handeln immer dann hoheitlich, wenn eine öffentlich-rechtliche Rechtsgrundlage zur Anwendung kommt und ein Subordinationsverhältnis besteht. Privatrechtlich handeln Bundesorgane demnach immer dann, wenn sie letztlich wie Private auftreten, so dass insbesondere kein Subordinationsverhältnis besteht. Beispiele privatrechtlicher Tätigkeiten durch Bundesorgane sind etwa das Beschaffen von Büromaterial, der Abschluss von Werkverträgen für die Errichtung öffentlicher Bauten oder die Vermietung von Liegenschaften.

- Im Folgenden geht es nun darum, die spezifisch für Bundesorgane bei der Ausübung ihrer hoheitlichen Aufgaben zum Zuge kommenden Vorgaben zu erörtern, wobei – auf der Grundlage einiger Bemerkungen über die Verantwortlichkeiten (I.) – zwischen der Notwendigkeit einer gesetzlichen Grundlage (II.), der Bekanntgabe von Personendaten (III.) sowie spezifischen Bearbeitungsvorgaben (IV.) unterschieden werden kann.

Die in Art. 25 DSG aufgeführten Rechte Dritter werden in einem eigenen Abschnitt (3. Kap.) erörtert, zusammen mit den sonstigen Rechten Betroffener.

I. Datenschutzrechtliche Verantwortung (Art. 16, 10a DSG)

Fall 10:
Das verantwortliche Bundesorgan möchte Daten per Fax an eine andere Behörde übermitteln. Worauf muss es achten und wer trägt die Verantwortung für die Datenübermittlung?

Nach **Art. 16 DSG** ist für die Einhaltung der Gesetzgebung über den Datenschutz, immer das **Bundesorgan verantwortlich**, welches **gestützt auf gesetzliche Grundlagen Personendaten bearbeitet oder bearbeiten lässt**.

Bearbeiten **Bundesorgane Personendaten zusammen** mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, kann der Bundesrat die Kontrolle und Verantwortung für den Datenschutz besonders regeln (**Art. 16 Abs. 2 DSG**). In der Regel bleiben aber die datenbearbeitenden Organe selbst für die Einhaltung der Gesetzgebung über den Datenschutz verantwortlich.

Als **Bundesorgane** gelten alle Behörden und Dienststellen des Bundes, sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind (**Art. 3 lit. h DSG**).

Das **Regierungs- und Verwaltungsorganisationsgesetz (RVOG)** und die dazugehörige Verordnung (RVOV) sind die massgebenden Rechtsgrundlagen für die Organisation und Zuständigkeit der Bundesverwaltung.
Obwohl die Organisation der Bundesverwaltung reglementiert ist, wird die Zuordnung der datenschutzrechtlichen Verantwortlichkeit zum Teil nicht immer einfach sein. **In der Regel** wird aber das **verantwortliche Organ mit dem Inhaber einer Datensammlung** (Art. 3 lit. i DSG) **identisch** sein, weil sich die datenschutzrechtliche Verantwortung in erster Linie aus der Kompetenz und der Aufgabe der Datenbearbeitung ableitet.

Wie sich schon aus dem Begriff der Verantwortung erschliesst, hat das zuständige Bundesorgan **umfassend** für die **Einhaltung** der **datenschutzrechtlichen Anforderungen** zu **sorgen**. So muss die Behörde dafür sorgen, dass die Art und Weise des Bearbeitens die Betroffenen zu keinem Zeitpunkt in ihrer Persönlichkeit verletzt und damit umfassend alle datenschutzrechtlichen Vorgaben beachtet und eingehalten werden.
Dieser Grundsatz gilt auch, wenn das Bundesorgan Dritte als Hilfspersonen beizieht oder die Datenverarbeitung vollständig ausgelagert wird (vgl. **Art. 10a DSG**, sog. **Outsourcing**): Auch dann bleibt das zuständige Bundesorgan verantwortlich und muss sicherstellen, dass alles zur Wahrung der Persönlichkeitsrechte der Betroffenen getan wird, was es selbst tun müsste und alles unterlassen wird, was es selber auch unterlassen müsste. Die Rechtsposition der Betroffenen darf sich durch die Auslagerung einer Datenbearbeitung in keiner Weise verschlechtern.

Art. 10a Abs. 1 DSG erlaubt grundsätzlich ein solches **Outsourcing**. Allerdings muss das beauftragende Bundesorgan dafür sorgen, dass die **Datenbearbeitung allen einschlägigen gesetzlichen Vorgaben genügt**, die es auch selbst zu beachten hätte (Art. 10a Abs. 1 lit. a DSG). Insbesondere muss sich der Auftraggeber vergewissern, dass die Anforderungen an die Datensicherheit (2. Kap. A.VII.) eingehalten werden, so dass die notwendigen technischen und organisatorischen Massnahmen ergriffen werden, damit die Personendaten vor jeder unbefugten Bearbeitung geschützt werden. Dem **Auftraggeber** obliegt hier also eine **umfassende Sorgfaltspflicht**.
Damit tatsächlich die Einhaltung dieser Vorgaben sichergestellt sein kann, ist in der Regel der Abschluss eines entsprechenden **Vertrages** notwendig, in dem der Auftragnehmer die einschlägigen Verpflichtungen eingeht (vgl. in diesem Zusammenhang auch die Checklisten für das Outsourcing auf www.dsb.zh.ch/themen.php?action=list&themesid=212&zoom_query=Outsourcing). In einer solchen Vereinbarung sind in der Regel etwa folgende Aspekte zu berücksichtigen:

- genauer Umfang der Datenbearbeitung durch den Auftragnehmer bzw. genaue Bezeichnung der Dienstleistung;
- Zugriff auf die Daten;
- Fragen der Bekanntgabe;

- verwendete Technologie, Datensicherheit und Sicherheitskonzept;
- Archivierung;
- Geheimhaltungspflichten;
- Kontrolle der Einhaltung der Vorgaben und ggf. Berichts- und Informationspflichten.

Trifft das **Bundesorgan nicht die sich nach den Umständen aufdrängenden Vorkehrungen**, damit der Auftragnehmer die einschlägigen gesetzlichen Verpflichtungen auch tatsächlich einhält, liegt eine **Persönlichkeitsverletzung durch das betreffende Bundesorgan** vor. Denn diesfalls geht es um eine Bekanntgabe von Personendaten ohne Beachtung der hierfür einschlägigen rechtlichen Voraussetzungen. Fraglich ist, ob die Verantwortlichkeit des Bundes auch dann begründet wird, wenn es zwar alle notwendigen Massnahmen ergriffen hat, der Auftragnehmer aber gleichwohl gegen eine der einschlägigen gesetzlichen Vorgaben verstösst. Nach der hier vertretenen Ansicht ist auch in einem solchen Fall die Verantwortlichkeit des Bundesorgans zu bejahen, denn letztlich muss es ihm zugerechnet werden, wenn der Auftragnehmer sich nicht an die gesetzlichen Vorgaben hält. Insofern kann man bei Art. 10a Abs. 1 lit. a DSG durchaus von einer „Erfolgspflicht" sprechen.
Zu beachten ist jedenfalls, dass das Outsourcing immer dann ausgeschlossen ist, wenn ihm gesetzliche (oder vertragliche) Geheimhaltungspflichten entgegenstehen (Art. 10 Abs. 1 lit. b DSG). Beispiele sind etwa das Fernmeldegeheimnis (Art. 45c FMG) oder das Bankgeheimnis. Grundsätzlich grösste ist Zurückhaltung beim Outsourcing ins Ausland geboten, da die effektive Einhaltung der genannten gesetzlichen Vorgaben hier in der Regel im Konflikt- oder Problemfall auf erhebliche Schwierigkeiten stossen kann.

Lösung Fall 10:
Bei der Datenübermittlung per Fax ist nicht auszuschliessen, dass das Dokument an den falschen Ort oder in „falsche" Hände gelangt. Der Absender trägt die Verantwortung für die Übermittlung. Er hat daher alle Vorkehrungen zu treffen, dass die Art und Weise der Datenübermittlung den Anforderungen des DSG entspricht, wozu auch gehört, dass er sich versichern muss, dass das Fax tatsächlich nur dem Adressaten zugänglich ist. Grundsätzlich empfiehlt es sich, den Empfänger zuvor zu unterrichten, damit der Zugang sichergestellt werden kann. Besonders schützenswerte Personendaten sollten nur dann per Fax übermittelt werden, wenn dies tatsächlich notwendig ist und der „richtige Empfang" mit Sicherheit überprüft wird. Ggf. kann sich eine verschlüsselte Übermittlung aufdrängen. Letzteres gilt auch für die Übermittlung besonders schützenswerter Personendaten per Mail.

II. Legalitätsprinzip (Art. 17, 17a, 18 DSG)

1. Grundsatz

Fall 11 (vgl. BGE 124 I 176):
Die Behörde S möchte, gestützt auf eine gesetzliche Grundlage (in einem Bundesgesetz), die Steuerdaten von Herrn B an eine andere Behörde bekannt gegeben. Herr B ist damit nicht einverstanden und verlangt die Sperrung der Bekanntgabe seiner Steuerdaten. Wird er mit seinem Anliegen erfolg haben?

Fall 12 (vgl. VPB 62.43):
Die kantonale Steuerbehörde X gelangt mit dem Begehren an das Bundesamt für Migration, ihr sämtliche im Kanton wohnhafte Asylbewerber bekannt zugeben (Liste der Asylbewerber). Die kantonale Steuerbehörde X benötigt diese Liste zu Steuerzwecken und namentlich zur Bekämpfung der Schwarzarbeit. Weder die Verordnung vom 18. November 1992 über das automatisierte Personenregistratursystem AUPER (AUPER-V, SR 142.315) noch die Steuergesetzgebung oder die Sozialversicherungsgesetzgebung enthalten Vorschriften, welche eine ausdrückliche Ermächtigung des Bundesamts für Migration als Inhaber der Asylbewerberdaten zur Datenbekanntgabe in grossem Umfang (Listen) an andere Behörden regeln. Darf das Bundesamt für Migration die Datenbekanntgabe trotzdem vornehmen?

Art. 17 DSG präzisiert den bereits in Art. 4 Abs. 1 DSG enthaltenen Grundsatz der Rechtmässigkeit (2. Kap. A.II.) für die Bundesorgane dergestalt, dass diese Personendaten – unabhängig von Verfahren und eingesetzten Mitteln (Art. 3 lit. e DSG) und unabhängig von der Art der bearbeiteten Daten (Art. 3 lit. a-d DSG) – nur dann bearbeiten dürfen, wenn hierfür eine **gesetzliche Grundlage** besteht. M.a.W. genügt es für die Rechtmässigkeit einer solchen Bearbeitung gerade nicht, dass ihr keine Rechtsnormen entgegenstehen, sondern die **Bearbeitung muss vielmehr ausdrücklich in einem Gesetz** vorgesehen sein.

Das bereits in der **Bundesverfassung** (Art. 5 Abs. 1 BV sowie Art. 36 Abs. 1 BV für Grundrechtseinschränkungen) vorgesehene **Legalitätsprinzip** wurde somit für die Bundesorgane explizit in das Datenschutzgesetz aufgenommen, wodurch ausdrücklich auf das **Prinzip der Spezialermächtigung** verwiesen wird. Daher können sich Bundesorgane grundsätzlich nicht auf das DSG als Rechtsgrundlage für eine Datenbearbeitung stützen, sondern für das Bearbeiten von Personendaten bedarf es einer bereichsspezifischen Rechtsgrundlage. Nur ausnahmsweise können sich Bundesorgane direkt auf das DSG stützen (vgl. Art. 17a, Art. 19, Art. 22 DSG). **Fehlt** eine solche **Rechtsgrundlage** und ist keine Ausnahmeregelung des DSG anwendbar, ist das Bearbeiten von Personendaten **widerrechtlich**.

Unter **gesetzliche Grundlage** im Sinne des Art. 17 Abs. 1 DSG ist ein **Gesetz im materiellen Sinn** zu verstehen, so dass die Bearbeitung von Personendaten in einer generell-abstrakten Norm vorgesehen sein muss. Bei der gesetzlichen Grundlage kann es sich um eine Verfassungs- oder Gesetzesbestimmung, um eine gestützt darauf erlassene Verordnungsnorm oder einen völkerrechtlichen Vertrag handeln (BBl 1988 II 467). Unter einer gesetzliche Grundlage versteht man also nicht nur ein **Gesetz im formellen Sinn**, wie dies in Art. 17 Abs. 2 DSG für die besonders schützenswerten Personendaten verlangt wird (2. Kap. C.II.2.). Auch eine Verordnung ist eine generell-abstrakte Rechtsnorm und stellt eine gesetzliche Grundlage i.S.v. Art. 17 Abs. 1 DSG dar. Eine Ausnahme sind Verwaltungsverordnungen, ihnen kommt in der Regel keine Rechtssatzqualität zu.
Sofern ein **schwerer Eingriff in die Persönlichkeitsrechte** oder die Privatsphäre durch die Datenbearbeitung impliziert ist, muss jedoch – unabhängig von der Frage, ob es um die Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen geht – ein **Gesetz im formellen Sinn** vorliegen, wie sich aus **Art. 36 Abs. 1 S. 2 BV** ergibt, wonach „schwerwiegende Einschränkungen" von Grundrechten im Gesetz selbst vorgesehen sein müssen. Diese Voraussetzung kann etwa dann gegeben sein, wenn nicht die Art der Daten, sondern die Form ihrer Beschaffung einen besonders schweren Eingriff in die Persönlichkeitsrechte darstellt (z.B. im Falle geheimer Überwachung).

Damit die somit jedenfalls erforderliche **gesetzliche Grundlage als genügend** erachtet werden kann, muss sie mindestens den Zweck, die beteiligten Bundesorgane sowie das Ausmass der Datenbearbeitung in den Grundzügen festlegen. Allerdings sind an eine solche gesetzliche Grundlage keine allzu hohen Anforderungen zu stellen, da die Datenbearbeitung durch die Bundesverwaltung sehr vielfältig ausfallen kann. Es kann daher bereits genügen, wenn ein sachlicher Zusammenhang zwischen der Datenbearbeitung und den jeweiligen Aufgaben des Bundesorgans besteht (BBl 1988 II 467).
Eine gesetzliche Grundlage für Bundesorgane ist unter folgenden Voraussetzungen **hinreichend bestimmt** (vgl. EDÖB, 11. Tätigkeitsbericht, 13):

- Definition des Bearbeitungszwecks;
- Umschreibung des Umfangs der Datenbearbeitung in groben Zügen;
- Festhalten der an der Datenbearbeitung Beteiligten sowie
- Aufführen der Kategorien der bearbeiteten Daten bei besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen (s. auch 2. Kap. C.II.2.).

Allerdings hängt der im **Einzelnen zu fordernde Grad der Bestimmtheit** von den **Umständen des Einzelfalls** und damit verschiedenen Kriterien ab, so insbesondere der Schwere des Eingriffs in die Persönlichkeitsrechte, der Art der bearbeiteten Daten, der Kreis der betroffenen Personen sowie der Komplexität der zu treffenden Entscheidung (BBl 1988 II 467).

Als Beispiel für eine gesetzliche Grundlage zur Bearbeitung von Personendaten sei nachfolgend Art. 96b des Arbeitslosenversicherungsgesetzes (AVIG, SR 837.0) aufgeführt, der die Bearbeitung von Personendaten für eine Reihe von Aufgaben vorsieht.

Art. 96b AVIG, Bearbeiten von Personendaten

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

a. Versicherte, die Versicherungsleistungen beanspruchen, zu erfassen, zu vermitteln und zu beraten;

b. Leistungsansprüche zu beurteilen sowie Leistungen zu berechnen, zu gewähren und mit Leistungen anderer Sozialversicherungen zu koordinieren;

c. Beitragsansprüche zu beurteilen sowie Beiträge zu berechnen, zu gewähren und deren Verwendung zu kontrollieren;

d. Versicherungsbeiträge an andere Sozialversicherungen zu erheben;

e. Quellensteuern zu erheben;

f. arbeitsmarktliche Massnahmen durchzuführen;

g. der Versicherung zustehende Ansprüche geltend zu machen;

h. die Aufsicht über die Durchführung dieses Gesetzes auszuüben;

i. Statistiken zu führen;

j. die Versichertennummer der AHV zuzuweisen oder zu verifizieren.

Auch ein Gesetz, das vor Inkrafttreten des Datenschutzgesetzes erlassen wurde, kann als gesetzliche Grundlage für die Bearbeitung von Personendaten durch Bundesorgane genügen (vgl. BGE 124 I 176, E. 5.bb).

Beim Erlass bereichsspezifischer Normen ist der Gesetzgeber grundsätzlich nicht an die im DSG verankerten Grundsätze gebunden. Damit kann der Gesetzgeber in **bereichsspezifischen Rechtsgrundlagen von gewissen allgemeinen Prinzipien oder Wertungen des Datenschutzgesetzes abweichen,** so dass einzelnen Bestimmungen des DSG keine eigenständige materielle Bedeutung mehr zukommt (BGE 126 II 126 E. 5b. und 5c; BGE 2A.534/2001, E.5). Soweit also z.B. ein Spezialgesetz ein Bundesorgan uneingeschränkt zur Bekanntgabe bestimmter Daten verpflichtet, stellt dies eine genügende Rechtsgrundlage dar, auch wenn einzelnen Grundsätzen des DSG nicht entsprochen wird. Dieser Grundsatz ergibt sich schon aus der Gleichrangigkeit gesetzlicher Normen. Allerdings ist in Bezug auf solche Abweichungen Folgendes zu beachten:

- Erstens können sie nur in einem **Gesetz im formellen Sinn** erfolgen, da das DSG als Bundesgesetz im Rang über Verordnungen steht.

- Zweitens sind die allgemeinen im DSG formulierten Grundsätze immer dann neben den spezialgesetzlichen Grundlagen zu beachten, soweit diese die Datenbearbeitung bzw. gewisse Aspekte derselben **nicht abschliessend regeln**.

- Drittens schliesslich sind im Sinne der Einheitlichkeit der Rechtsordnung bei der **Auslegung** der bereichsspezifischen Bestimmungen die **Grundsätze und die Prinzipien des DSG** zu berücksichtigen (BGE 126 II 126, E. 5.b. und 5.c.).

Lösung Fall 11 (vgl. BGE 124 I 176):
Herr B wird mit seinem Anliegen keinen Erfolg haben: Sofern für diese Bekanntgabe eine gesetzliche Grundlage in einem Bundesgesetz besteht, hat der Steuerpflichtige aufgrund des DSG keinen Anspruch darauf, die Bekanntgabe seiner Steuerdaten zu sperren. Diesfalls können und müssen die Daten auch gegen seinen Willen bekannt gegeben werden. Ein Gesetz, welches eine Behörde uneingeschränkt zur Bekanntgabe bestimmter Informationen verpflichtet, stellt eine Rechtsgrundlage dar, welche auch im datenschutzrechtlichen Sinne die Bekanntgabe zulässt.

Lösung Fall 12 (vgl. VPB 62.43):
Die systematische Bekanntgabe solcher Listen von Asylbewerbern die Steuerbehörden ist nur bei Vorliegen einer gesetzlichen Grundlage zulässig, die eine solche Bekanntgabe ausdrücklich vorsieht. Da eine solche nach dem Sachverhalt nicht gegeben ist, darf das Bundesamt für Migration die oben genannte

Datenbekanntgabe nicht vornehmen. Von dieser Konstellation zu unterscheiden ist die Amtshilfe im Einzelfall im Rahmen von Art. 19 Abs. 1 und 4 DSG sowie im Rahmen sektorieller Amtshilfevorschriften. Diese kann unter den in diesen Bestimmungen aufgeführten Voraussetzungen (2. Kap. C.III.) zulässig sein, da nur die Datenbekanntgabe im Einzelfall zur Debatte steht.

2. Besonders schützenswerte Personendaten und Persönlichkeitsprofile

Gemäss Art. 17 Abs. 2 DSG muss sich jede Bearbeitung von **besonders schützenswerten Personendaten oder Persönlichkeitsprofilen** (vgl. für eine Definition dieser beiden Begriffe Art. 3 lit. c sowie lit. d DSG) durch Bundesorgane grundsätzlich auf ein **Gesetz im formellen Sinn** – also in der Regel ein Bundesgesetz (Art. 3 lit. j DSG) – abstützen.

Daher bedarf etwa eine Datenbekanntgabe immer dann einer ausdrücklichen Regelung in einem Gesetz im formellen Sinn, wenn unter verschiedenen Behörden und zu verschiedenen Bearbeitungszwecken regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile ausgetauscht werden. Erhalten einzelne Behörden mittels Abrufverfahren Zugriff auf diese Daten, muss dieser Umstand ausdrücklich erwähnt und die berechtigte Behörde bezeichnet werden. Wird in diesem Zusammenhang ein grosses und verzweigtes EDV-System verwendet, muss auch dies im Gesetz im formellen Sinn ausdrücklich geregelt werden. Wenn sich gewisse Grundrechtseingriffe nur zusammen mit Schutzauflagen als grundrechtskonform erweisen sollten, sind auch diese Schutzauflagen in dem entsprechenden Gesetz im formellen Sinn zu regeln (vgl. VPB 60.77)

In den in **Art. 17 Abs. 2 lit. a-c DSG** abschliessend aufgezählten **Ausnahmefällen** kann aber auf eine Grundlage in einem Gesetz im formellen Sinn verzichtet werden:

- Gemäss **Art. 17 Abs. 2 lit. a DSG** kann ausnahmsweise eine Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen ohne eine Grundlage in einem Gesetz im formellen Sinn stattfinden, wenn dies für eine in einem **Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich** ist. Es müssen also die Bedingung der Unentbehrlichkeit für die Aufgabenerfüllung sowie die der klaren Aufgabenbeschreibung in einem Gesetz im formellen Sinn erfüllt sein. Unentbehrlichkeit kann nur dann angenommen werden, wenn die Aufgabe ohne die Bearbeitung der fraglichen Daten unmöglich wäre. Es darf sich bei Art. 17 Abs. 2 lit. a DSG nur um eine Datenbearbeitung in Einzelfällen handeln.

- Ausnahmsweise und ebenfalls nur in Einzelfällen kann der Bundesrat eine Datenbearbeitung bewilligen, sofern die Rechte der betroffenen Person nicht gefährdet sind (**Art. 17 Abs. 2 lit. b DSG**).

- Beim Vorliegen einer **Einwilligung der betroffenen Person** im Einzelfall kann ebenfalls auf eine Grundlage in einem Gesetz im formellen Sinn verzichtet werden (**Art. 17 Abs. 2 lit. c DSG, erster Fall**). Eine Einwilligung ist nur dann gültig, wenn die betroffene Person freiwillig einwilligt und sie weiss, wozu sie einwilligt. Sie muss also rechtzeitig und umfassend informiert werden. Ungenügend sind sog. Pauschalermächtigungen; diese schaffen keine genügende Transparenz. Die Einwilligung muss verweigert oder nachträglich widerrufen werden können. Sie kann schriftlich oder mündlich erfolgen und ist an keine bestimmte Form gebunden.

- Hat die betroffene Person ihre Daten allgemein zugänglich gemacht (z.B. durch Veröffentlichung eines Buches oder über eine Medienmitteilung) und eine Bearbeitung nicht ausdrücklich untersagt (Art. 17 Abs. 2 lit. c. DSG, zweiter Fall), kann auf eine Grundlage in einem Gesetz im formellen Sinn zur Bearbeitung der Daten verzichtet werden.

Neben den oben genannten Ausnahmefällen sind auch die ernsten, unmittelbaren und nicht anders abwendbare Fälle vom Erfordernis der Grundlage in einem Gesetz im formellen Sinn ausgenommen (Art. 36

Abs. 1 Satz 3 BV). Diese **sog. polizeiliche Generalklausel** kann aber nur dann greifen, wenn die öffentliche Ordnung und fundamentale Rechtsgüter des Staates oder Privater gegen schwere und unmittelbar drohende Gefahren zu schützen sind. Sie ist restriktiv anzuwenden.

3. Insbesondere: die Beschaffung von Personendaten

Auch die **Beschaffung von Personendaten** – die erste Phase und die Voraussetzung jeder weiteren Datenbearbeitung (vgl. Art. 3 lit. e DSG) – ist nur unter der Voraussetzung einer genügenden gesetzlichen Grundlage zulässig; insofern gelten die soeben erörterten allgemeinen Grundsätze. Das Erfordernis einer gesetzlichen Grundlage gilt auch dann, wenn eine **Datenbeschaffung bei einer anderen Verwaltungsstelle** erfolgt; Ausnahmen sind grundsätzlich (abgesehen von spezialgesetzlichen Bestimmungen) nur unter den Voraussetzungen des Art. 19 Abs. 1 lit. a, b, d DSG zulässig.
Art. 18 DSG und **Art. 24 VDSG** enthalten darüber hinaus und in Ergänzung zu den allgemeinen Grundsätzen von Art. 4 f. DSG und Art. 17 DSG weitere Vorgaben über die **Information der Betroffenen beim Beschaffen von Personendaten**. Diese sollen es den betroffenen Personen ermöglichen, Grundlagen und Ausmass der vorgesehenen Beschaffung zu beurteilen und gestützt darauf entscheiden zu können, ob sie ihre Daten zur Verfügung stellen wollen oder nicht (sofern keine gesetzliche Pflicht zur Auskunftserteilung besteht).
Art. 18 DSG behandelt das **systematische Erheben von Daten** – welches vorliegt, wenn die Daten **methodisch, organisiert und strukturiert** (insbesondere mittels Fragebogen) **beschafft** werden – und sieht dafür besondere **Orientierungspflichten** vor:

- Die betroffene Person muss den **Bearbeitungszweck** kennen. Nur dann ist es ihr möglich, allfällige Risiken richtig einzuschätzen.

- Damit die betroffene Person die Rechtmässigkeit der Datenbearbeitung beurteilen kann, müssen ihr die **gesetzlichen Grundlagen**, welche die Bearbeitung vorsieht, bekannt gegeben werden.

- Schliesslich sind die **Kategorien der an der Datensammlung Beteiligten und der Datenempfänger** bekannt zu geben (nicht aber die einzelnen Beteiligten, was zu einem unverhältnismässigen Aufwand führen würde).

Weiter hat das Bundesorgan gemäss **Art. 24 Abs. 1 VDSG** die betroffene Person über eine allenfalls bestehende **Verpflichtung zur Auskunftserteilung** und die Folgen der Auskunftsverweigerung oder einer falschen Antwort zu informieren. Ansonsten ist die befragte Person bei systematischen Erhebungen von Personendaten mittels Fragebogen auf die **Freiwilligkeit der Auskunftserteilung** hinzuweisen (**Art. 24 Abs. 2 VDSG**).

4. Automatisierte Datenbearbeitung im Rahmen von Pilotprojekten (Art. 17a DSG)

Art. 17a DSG **ermöglicht** es dem **Bundesrat**, während einer **zeitlich beschränkten Versuchsphase** die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen im Rahmen von **Pilotversuchen** zu bewilligen, **bevor** ein **Gesetz im formellen Sinn in Kraft** getreten ist.

Gemäss Art 17a Abs. 1 DSG kann demnach – wenn zur Umsetzung einer bestimmten Bearbeitung oder eines Informatiksystems eine **Testphase zwingend erforderlich** ist, die entsprechenden Aufgaben in einem Gesetz im formellen Sinn festgelegt sind und ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden – auf eine **Grundlage in einem Gesetz im formellen Sinn,** für eine Pilotphase **temporär verzichtet** werden.

Art. 17a DSG stellt somit eine **Ausnahme vom Erfordernis eines Gesetzes im formellen Sinn** für die **Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen** dar.

Der Hintergrund des Art. 17a DSG ist darin zu sehen, dass vor dem Erlass eines Gesetzes im formellen Sinn genügend Erfahrungen mit dem praktischen Betrieb einer technischen Lösung gesammelt werden können.

Auf die Ausnahme des **Art. 17a DSG** kann nur bei Vorliegen von **drei kumulativen Voraussetzungen** zurückgegriffen werden:

- Die **Aufgaben**, die die Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen erforderlich machen, sind in einem **Gesetz im formellen Sinn** geregelt.

- Es müssen ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzung getroffen werden.

- Die **praktische Umsetzung** der Datenbearbeitung erfordert **zwingend eine Testphase** vor dem Inkrafttreten des Gesetzes.

  Art. 17a Abs.2 DSG legt die Kriterien fest, nach welchen zu beurteilen ist, ob eine **Testphase zwingend erforderlich** ist:

  - Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen (z.B. Rückgriff auf Software, die bisher noch nicht mit realen Daten benutzt wurden).
  - Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss.
  - Die Bearbeitung erfordert die Übermittlung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an kantonale Behörden mittels Abrufverfahren.

Gemäss **Art. 17a Abs. 1 DSG** muss der Bundesrat bevor er eine solche Testphase bewilligt, eine **Stellungnahme des EDÖB** einholen. **Art. 27** und **27a VDSG** umschreiben das **Verfahren bei der Bewilligung von Pilotversuchen** näher.

Die **Testphase** darf nicht beliebig lange dauern, sondern ist **zeitlich beschränkt**. Das zuständige Bundesorgan muss dem Bundesrat **innert zwei Jahren** nach Inbetriebnahme das Pilotsystems einen **Evaluationsbericht** vorlegen. Darin muss es die Fortführung oder die Einstellung der Bearbeitung vorschlagen (Art. 17a Abs. 4 DSG). Der Evaluationsbericht muss eine vollständige Bilanz über die Testphase ziehen; nicht nur die Vorteile, sondern auch die Nachteile müssen dargelegt werden. Gemäss Art. 17a Abs. 5 DSG muss die automatisierte Datenverarbeitung in jedem Fall **abgebrochen** werden, wenn **innert 5 Jahren** nach der Inbetriebnahme des Pilotsystems kein Gesetz im formellen Sinn in Kraft getreten ist, welches die erforderliche Rechtsgrundlage enthält.

Im Rahmen von Pilotprojekten wurde bislang vor allem die Verwendung von biometrischen Mitteln getestet. So wurden beispielsweise seit 2006 im Hinblick auf die Einführung des biometrischen Schweizer Passes im Rahmen eines Pilotprojekts solche Pässe auf freiwilliger Basis ausgestellt.

5. Fazit

Zusammenfassend ist somit festzuhalten, dass in all denjenigen Konstellationen, in denen ein Bundesorgan mit der Frage konfrontiert ist, ob eine bestimmte Datenbearbeitung, insbesondere eine Datenbekanntgabe, zulässig ist, grundsätzlich in folgenden Schritten vorzugehen ist:

- Zunächst ist jeweils die Frage zu klären, auf welcher **Rechtsgrundlage** die betreffende Datenbearbeitung erfolgen darf. **Fehlt** eine solche **gesetzliche Grundlage** und ist keine Ausnahmeregelung des DSG (z.B. Art. 19 Abs. 1 DSG)

einschlägig, ist das Bearbeiten von Personendaten **widerrechtlich** und somit zu unterlassen.

- Werden **besonders schützenswerte Personendaten** oder **Persönlichkeitsprofile** bearbeitet, ist – es sei denn, eine der Ausnahmen des Art. 17 Abs. 2 DSG liege vor – eine Grundlage in einem **Gesetz im formellen Sinn** notwendig.

- Besteht für die betreffende Datenbearbeitung eine **Rechtsgrundlage in einem Gesetz im formellen Sinn**, so ist diese **vollumfänglich einschlägig** und massgebend. Allerdings ist soweit auf die allgemeinen Grundsätze des DSG zurückzugreifen, als die **spezialgesetzliche Regelung** die betreffende Bearbeitung nur **unvollständig** regelt. Im Zweifel ist die Spezialregelung im Übrigen **im Einklang mit den allgemeinen datenschutzrechtlichen Grundsätzen auszulegen**.

- Besteht für die betreffende Datenbearbeitung eine **Rechtsgrundlage in einem Gesetz im materiellen Sinn**, so ist dieses soweit massgeblich, wie es mit den **datenschutzrechtlichen Grundsätzen in Einklang** steht; diese sind m.a.W. jeweils zusätzlich bei der Prüfung der Rechtmässigkeit der Bearbeitung zu berücksichtigen. Im Falle der Durchbrechung allgemeiner datenschutzrechtlicher Grundsätze des DSG durch ein Gesetz im materiellen Sinn ist dieses daher insoweit unangewandt zu lassen, es sei denn, diese Durchbrechung beruhe ihrerseits auf einem Gesetz im formellen Sinn bzw. ist in diesem bereits angelegt.

- Schliesslich sei noch daran erinnert, dass auch und gerade im Zuge der Massgeblichkeit der Spezialgesetze der **Grundsatz der Verhältnismässigkeit** (2. Kap. A.IV.) – der nicht nur im DSG, sondern bereits in der Bundesverfassung verankert ist – jeweils gesondert zu prüfen ist, so dass eine Datenbearbeitung keinesfalls gegen diesen – allerdings „dehnbaren" – Grundsatz verstossen darf.

- Deutlich wird damit, dass sich die **Zulässigkeit einer konkreten Datenbearbeitung** in aller Regel erst auf der Grundlage und nach der Analyse der für die jeweilige Fallgestaltung einschlägigen **Spezialgesetzgebung** ergibt, die somit von entscheidender Bedeutung ist. Vor diesem Hintergrund wird auch deutlich, dass das **Datenschutzrecht eine Querschnittsmaterie** darstellt, das letztlich in (fast) allen Bereichen staatlicher Tätigkeiten regelungsbedürftig ist und auch geregelt wird.

Dies impliziert aber auch eine gewisse **Unübersichtlichkeit des Datenschutzrechts**, da die Rechtsgrundlagen in den verschiedenen Rechtsgebieten und damit auch die Anforderungen an die Zulässigkeit von Datenbearbeitungen in allen Spezialgesetzen und dem dazugehörigen Verordnungsrecht „verstreut" sind, so dass es nicht immer einfach ist, sich einen Überblick über die für eine konkrete Situation einschlägigen Vorgaben zu verschaffen. Im Übrigen sind die **Rechtsgrundlagen mitunter auch recht unterschiedlich** ausgestaltet, so dass es eine Vielzahl von verschiedenen „Kategorien" bzw. Systemen von Vorgaben für die Zulässigkeit unterschiedlicher Datenbearbeitungen gibt.

Diese Situation ist zweifelsohne insofern systembedingt, als erst durch die Einfügung von Rechtsgrundlagen in den verschiedenen Spezialgesetzen eine hinreichende demokratische Legitimierung des mit jeder Datenbearbeitung verbundenen staatlichen Eingriffs sichergestellt werden kann. Auch ist die unterschiedliche Ausgestaltung der Rechtsgrundlagen schon deshalb notwendig, weil es um unterschiedliche Daten und unterschiedliche Zielsetzungen geht. Gleichwohl bringt dieses System insgesamt gerade auch für den betroffenen Bürger eine gewisse Intransparenz mit sich, ist es für ihn doch mitunter sehr schwierig zu

eruieren, ob und inwieweit ihn betreffende Daten bearbeitet werden dürfen. Es wäre daher zumindest erwägenswert zu untersuchen, ob es möglich wäre, die in den verschiedenen Spezialgesetzen „verstreuten" datenschutzrechtlichen Bestimmungen in einem einzigen Rechtsakt zusammenzufassen (soweit die Bundesebene betroffen ist), der dann eben die Rechtsgrundlagen für die Datenbearbeitung in den verschiedenen Gebieten staatlicher Tätigkeiten enthielte. Auf diese Weise wäre es auch möglich, eine für alle Datenbearbeitungen einschlägigen „allgemeinen Teil" zu formulieren, bevor die spezifischen Voraussetzungen für die einzelnen Bereiche geregelt werden.

III. Bekanntgabe von Personendaten (Art. 19 DSG)

1. Allgemeines

Fall 13 (vgl. BGE 2A.424/2000):
Herr X, Schweizer Bürger heiratet im Sommer 2008 die jugoslawische Staatsangehörige Frau Y. Im August 2008 ersucht Herr X beim Departement des Innern des Kantons S um eine Aufenthaltsbewilligung für seine Ehefrau. Dieses Gesuch wird abgewiesen. Zur Begründung wird angeführt, der Ehefrau könne keine Aufenthaltsbewilligung erteilt werden, weil die Ehe nicht eingegangen worden sei, um eine Familiengemeinschaft zu begründen, sondern um die Wegweisung zu verhindern. Herr X erhebt gegen diesen Entscheid Beschwerde und macht u.a. geltend, das Departement des Innern des Kantons S habe Akten der Fremdenpolizei der Kantone Zürich und Aargau beigezogen (das Bundesamt für Migration stellte diese zur Verfügung). Herr X bringt vor, der Beizug von Befragungsprotokollen aus dem Asylverfahren, welche durch die Fremdenpolizei der genannten Kantone erstellt worden sind, verstosse gegen das Datenschutzrecht des Bundes. Die entsprechenden Protokolle seien einzig zur Verwendung im Asylverfahren aufgenommen worden und stünden unter der Hoheit des Bundesamtes für Migration. Hätten die Protokolle gemäss Art. 19 DSG verwendet werden dürfen?

Fall 14:
Der Schweizerische Nationalfonds zur Förderung der Wissenschaftlichen Forschung (SNF) entscheidet in über die Bewilligung und damit die Finanzierung von Anträgen zur Forschungsförderung. Im Rahmen der Erörterung der Frage, wie mit Verstössen gegen die Regeln der wissenschaftlichen Redlichkeit bei der Gesuchseingabe (z.B. Plagiate oder „Wiederverwendung" von Ideen Dritter) umzugehen ist, stellt sich der SNF die Frage, ob im Falle der Feststellung eines solchen Verstosses durch die zuständigen Gremien des SNF im Rahmen eines Gesuchsverfahren die Heimatuniversitäten der Gesuchsteller über den Vorfall regelmässig zu informieren sind. Schliesslich gehe es um grundlegende Regeln der wissenschaftlichen Arbeit, so dass zumindest die Universitätsrektoren bzw. ETH-Präsidenten über ein solches Fehlverhalten der an ihren Institutionen angestellten Personen informiert werden müssten, könnten diese Personen doch möglicherweise die ihnen anvertrauten Aufgaben nicht mehr kompetent wahrnehmen.

Die Bekanntgabe von Personendaten ist ein Unterfall der Bearbeitung von Personendaten (Art. 3 lit. e DSG, 1. Kap. D.), die insofern – etwa im Vergleich zur „amtsinternen" Bearbeitung – besondere Fragen aufwirft, als auf diese Weise Dritte (seien dies nun Private oder eine andere Verwaltungsstelle) Einsicht in die bei einem Bundesorgan vorhandenen bzw. von diesem beschafften Daten Einsicht erlangen. Vor diesem Hintergrund sieht **Art. 19 DSG** eine **spezifische Regelung** vor, an deren Massstab zu prüfen ist, ob eine **Bekanntgabe von Personendaten** durch ein Bundesorgan rechtmässig ist.

Der Umstand, dass eine Weitergabe von Personendaten an **Private** im Lichte des Persönlichkeitsschutzes problematisch ist bzw. sein kann, liegt auf der Hand. Aber auch die Weitergabe von Personendaten **zwischen staatlichen Organen** (Bundesorgane untereinander oder Bundesorgane und kantonale Organe) steht grundsätzlich in einem **Spannungsverhältnis mit dem Grundsatz der Zweckbindung** (werden doch Daten in aller Regel nicht im Hinblick auf eine Weitergabe gesammelt) und ggf. dem Legalitätsprinzip (muss doch jede Bearbeitung, auch die Bekanntgabe, auf einer gesetzlichen Grundlage beruhen). Grundsätzlich gilt daher ein **Grundsatz der Trennung bzw. Nichtverknüpfung der bei den verschiedenen staatlichen Organen vorhandenen Personendaten**. Zwar leisten Bund und Kantone (vgl. auch Art. 44 BV) und Bundesorgane untereinander gegenseitig **Amtshilfe** (worunter die gegenseitige Unterstützung von Verwaltungseinheiten, die nicht in einem Subordinationsverhältnis zueinander stehen, durch nicht verfahrensrechtlich geregelte Hilfeleistungen bei deren gesetzlicher Aufgabenerfüllung, zu verstehen ist); allerdings ist nach dem Gesagten auch bei der Bekanntgabe von Daten zwischen Verwaltungsbehörden untereinander, der **Grundsatz der Legalität** zu beachten, so dass sie schon nach Art. 13 BV i.V.m. Art. 36 BV einer gesetzlichen Grundlage

bedarf, im öffentlichen Interesse liegen und den Anforderungen des Verhältnismässigkeitsgrundsatzes entsprechen muss.
Insofern handelt es sich bei Art. 19 DSG um eine Art **allgemeine Amts- und Rechtshilfebestimmung** (BBl 1988 II 496). Amtshilfe darf nur im Einzelfall erfolgen und muss für den Empfänger für die Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Amtshilfe ist insofern Teil der Datenbekanntgabe gemäss Art. 19 DSG, als es sich um die Bekanntgabe von Personendaten an eine andere staatliche Stelle handelt. Die Amtshilfe bzw. die Datenbekanntgabe im Rahmen der Amtshilfe stellt aber wohlgemerkt nur einen Teil der in Art. 19 DSG geregelten Formen der Datenbekanntgabe dar.

Der **Anwendungsbereich des Art. 19 DSG** erstreckt sich sowohl auf den **Datenaustausch zwischen Bundesorganen untereinander** als auch auf die **Weitergabe von Daten an kantonale, kommunale oder ausländische Behörden sowie an Privatpersonen.**
Dabei wiederholt Art. 19 Abs. 1 DSG zunächst den sich bereits aus Art. 17 DSG ergebenden Grundsatz, dass eine Bekanntgabe nur erfolgen darf, wenn hierfür eine **Rechtsgrundlage im Sinne des Art. 17 DSG** vorliegt (2. Kap. C.II.1.). Diesem Aspekt des Art. 19 Abs. 1 DSG dürfte daher im Verhältnis zu Art. 17 Abs. 1 DSG keine eigenständige Bedeutung zukommen.

Die gesetzliche Grundlage – wie sie in Art. 19 DSG verlangt wird – muss sich **explizit und spezifisch auf die Datenbekanntgabe** beziehen, d.h. eine Ermächtigung (z.B. Art. 50a AHVG) oder Verpflichtung (z.B. Art. 91 Abs. 5 SchkG) zur Datenbekanntgabe enthalten. Eine allgemeine Kompetenz zur Datenbearbeitung i.S.v. Art. 17 DSG genügt für die Datenbekanntgabe nicht (BBl 1989 469), da sie nicht hinreichend genau die Art und Weise der Datenbearbeitung umschreibt (zu den Anforderungen an die Bestimmtheit einer gesetzlichen Grundlage bereits 2. Kap. C.II.1.).
Die Rechtsgrundlagen für die Bekanntgabe von Personendaten an Dritte können sehr unterschiedlich ausgestaltet sein. Insbesondere können sie eine **Pflicht** oder lediglich eine **Ermächtigung** zur Bekanntgabe beinhalten. Im letzteren Fall sind bei jeder Bekanntgabe jeweils noch die **allgemeinen datenschutzrechtlichen Grundsätze** (2. Kap. A.) zu beachten, wobei – neben der sich in der Spezialgesetzgebung findenden Kriterien – insbesondere folgende Gesichtspunkte von Bedeutung sind:

- Der Grundsatz von **Treu und Glauben** ist zu beachten, so dass etwa allgemeine Suchaktionen (*fishing expedition*) – auf die sich die Betroffenen nicht einstellen müssen – grundsätzlich unzulässig sind.
- Die Datenbekanntgabe muss den Anforderungen des **Verhältnismässigkeitsgrundsatzes** gerecht werden, so dass Personendaten z.B. in anonymisierter Form weiterzugeben sind, wenn es keiner Nennung bestimmter Personen bedarf, oder dass keine Daten „auf Vorrat" bekannt gegeben werden dürfen. Daten dürfen also grundsätzlich nur im tatsächlich notwendigen Umfang bekanntgegeben werden.
- Die Bekanntgabe muss grundsätzlich dem **Zweck der ursprünglichen Beschaffung** entsprechen. Einmal erhobene Daten dürfen nämlich nur zu Zwecken verwendet werden, die Grund für die ursprüngliche Beschaffung waren. Zweckidentität bzw. Zweckkompatibilität liegt vor, wenn die Weiterverwendung von Daten für die betroffene Person transparent bleibt (Art. 4 Abs. 3, 4 DSG, 2. Kap. A.V.). So bejahte das Bundesgericht etwa die Zweckidentität für den Fall der Weiterleitung von fremdenpolizeilich erstellten Asylakten im Hinblick auf die Verwendung in einem ausländerrechtlichen Verfahren, da sowohl das Asylrecht als auch das Ausländerrecht letztlich die Frage der Anwesenheitsberechtigung von Ausländern in der Schweiz betreffen (BG, Urt. v. 13.2.2001, 2A.424/2000, E. 2.d, Fall 13).
- Schliesslich müssen die von den Bundesorganen bekannt gegebenen **Daten richtig** sein (Art. 5 DSG, 2. Kap. A.VII.). In diesem Sinn ist das verantwortliche Bundesorgan gemäss **Art. 26 VDSG** verpflichtet, dem Datenempfänger die **Aktualität und die Zuverlässigkeit** der von ihm bekannt gegebenen Daten zu melden, soweit diese Informationen nicht aus den Daten selbst oder den Umständen ersichtlich sind.

Jedenfalls hat die **bekannt gebende Behörde** über die Datenbekanntgabe nach dem **für sie selbst massgeblichen Recht** zu entscheiden (VPB 65.52, E. 3).

Beispiele aus der Praxis:

- Für die Bekanntgabe von Personendaten über die einer Selbstregulierungsorganisation angeschlossenen Finanzintermediäre an in- und ausländische Behörden, insbesondere für das allgemeine Zugänglichmachen solcher Daten durch ein elektronisches Abrufverfahren, fehlt eine Rechtsgrundlage (VPB 68.92 Erw. 3).

- Die Bekanntgabe von Personendaten einer Mitarbeiterin im Rahmen eines Weiterbildungsseminars ist widerrechtlich, da kein Rechtsfertigungsgrund gemäss Art. 19 DSG gegeben ist (VPB 64.70).

Eine gesetzliche Grundlage ist in jedem Fall immer dann erforderlich, wenn die Datenbekanntgabe durch ein sog. **Abrufverfahren** erfolgt (**Art. 19 Abs. 3 DSG**). **Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile** dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein **Gesetz im formellen Sinne** dies ausdrücklich vorsieht.

Unter **Abrufverfahren** sind **automatisierte Verfahren** zu verstehen, die es dem informationssuchenden Organ ermöglichen, sich die gewünschte Information in einem existierenden Datenbestand selbst zu beschaffen bzw. eben „abzurufen", ohne dass die eigentlich bekannt gebende Behörde hier mitwirken muss bzw. die Abrufung überhaupt bemerkt. Es liegt auf der Hand, dass mit solchen Verfahren besondere Risiken verbunden sind, kann hier doch definitionsgemäss nicht mehr jeder Einzelfall analysiert werden.

Darüber hinaus gilt der **Grundsatz**, dass für die Bekanntgabe von Personendaten eine gesetzliche Grundlage bestehen muss (abgesehen von den soeben erwähnten Bekanntgaben durch ein Abrufverfahren), **nicht absolut**. Besteht keine gesetzliche Grundlage, ist die Bekanntgabe von Personendaten durch Bundesorgane gleichwohl möglich, wenn eine der in **Art. 19 Abs. 1 lit. a-d DSG** aufgeführten Konstellationen bzw. Voraussetzungen – die auch, mangels gegenteiliger Anhaltspunkte in Art. 19 Abs. 1 DSG, für die Bekanntgabe besonders schützenswerter Daten oder von Persönlichkeitsprofilen zum Zuge kommen können (so dass Art. 19 Abs. 1 DSG auch in dieser Hinsicht im Verhältnis zu Art. 17 DSG eine spezielle Regelung darstellt) – vorliegt:

- Die Daten sind für den **Empfänger im Einzelfall** zur **Erfüllung seiner gesetzlichen Aufgabe unentbehrlich (Art. 19 Abs. 1 lit. a DSG)**: Diese Konstellation betrifft den Sachverhalt, in dem der Empfänger seine gesetzliche Aufgabe ohne Datenbekanntgabe überhaupt nicht erfüllen könnte. Eine Bekanntgabe gestützt auf diese Bestimmung ist auf den Einzelfall beschränkt, und die Bekanntgabe muss für den Empfänger tatsächlich unentbehrlich sein. Umfassende bzw. systematische Datenbekanntgaben bei Vorliegen typisierter und nach allgemein-abstrakten Kriterien bestimmten Voraussetzungen sind daher nur gestützt auf eine ausdrückliche Rechtsgrundlage zulässig, können also nicht aufgrund dieser Bestimmung erfolgen.

  Auch bei einer nach Art. 19 Abs. 1 lit. a DSG erfolgenden Datenbekanntgabe sind selbstredend die **allgemeinen datenschutzrechtlichen Grundsätze** des Art. 4 DSG zu beachten, wobei dem Grundsatz der Zweckbindung und dem Verhältnismässigkeitsprinzip eine besondere Bedeutung zukommen dürfte. So darf – entsprechend dem Grundsatz der Zweckbindung – die Datenbekanntgabe nicht erfolgen, wenn sie mit dem Zweck der ursprünglichen Datenerhebung nicht vereinbar ist.
  Eine Datenbekanntgabe darf sodann nur auf **Anfrage** erfolgen, so dass die bekannt gebende Behörde andere Behörden nicht „spontan" informieren darf.

- Die **betroffene Person** hat im **Einzelfall eingewilligt (Art. 19 Abs. 1 lit. b DSG)**: Die Einwilligung kann grundsätzlich ausdrücklich oder stillschweigend erfolgen, wobei aber den Anforderungen des Art. 4 Abs. 5 DSG Rechnung zu tragen ist. Bei der Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen wird eine ausdrückliche Einwilligung verlangt (Art. 4 Abs. 5 S. 2 DSG, BBl 2003 2127, 2157).

  Eine unter Druck zustande gekommene Einwilligung ist ebenso ungültig, wie eine Einwilligung, welche abgegeben wurde, ohne dass die betroffene Person deren Tragweite und Risiken kannte. Allerdings ergibt sich aus einem Nachteil für die betreffende Person im Falle einer Verweigerung der Einwilligung noch nicht, dass die Einwilligung von vornherein unfreiwillig ist. Dies ist nur dann anzunehmen, wenn der Nachteil keinen Bezug zum Zweck der Bearbeitung hat oder diesem gegenüber unverhältnismässig ist (BBl 2003, 2127).

In eine unrechtmässige Datenbearbeitung kann nicht eingewilligt werden. Ebenso wenig kann eine Einwilligung eine gegen Treu und Glauben verstossende Datenbearbeitung rechtfertigen.

- Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt (Art. 19 Abs. 1 lit. c DSG).

- Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren (Art. 19 Abs. 1 lit. d DSG): Hier geht es letztlich um Fallgestaltungen, in denen die betroffene Person in rechtsmissbräuchlicher Art Angaben über sich selber verweigert, so dass eine Bekanntgabe von Personendaten auch ohne Rechtsgrundlage und ohne Einwilligung erfolgen kann. Es handelt sich in der Praxis meist um Fälle, in denen eine Person die Bekanntgabe der eigenen Daten verweigert, um einer Rechtspflicht wie etwa Alimentenzahlungen oder Sozialversicherungsbeiträgen zu entgehen. Vor der Datenbekanntgabe ist der Person die Gelegenheit zur Stellungnahme zu geben. In Ausnahmefällen kann darauf verzichtet werden.

Eine **weitere Ausnahme** vom Grundsatz der Notwendigkeit einer spezialgesetzlichen Grundlage für die Bekanntgabe von Personendaten ergibt sich aus **Art. 19 Abs. 2 DSG**: Danach dürfen die Bundesorgane **auf Anfrage** (womit regelmässige und systematische Bekanntgaben nicht gedeckt werden) die **sog. Stammdaten** (Name, Vorname, Adresse und Geburtsdatum einer Person) bekannt geben, ohne dass die Voraussetzungen von Art. 19 Abs. 1 DSG erfüllt sind. Die gesetzliche Grundlage für eine solche Bekanntgabe findet sich also in Art. 19 Abs. 2 DSG direkt, und auch die Anforderungen des Art. 19 Abs. 1 lit. a-d DSG müssen nicht erfüllt sein.

Der Hintergrund dieser Regelung ist darin zu sehen, dass gewisse Grundangaben zur Identifizierung einer Person, die ohnehin relativ allgemein bekannt sind und deren Bekanntgabe in der Regel keinen schweren Eingriff in die Persönlichkeitsrechte der Betroffenen darstellt, auf relativ einfache Weise in Erfahrung gebracht werden können sollen (BBl 1988 II 471).

Auch bei einer Datenbekanntgabe nach Art. 19 Abs. 2 DSG müssen die Bundesorgane aber den allfälligen **Schutzbedürfnissen einer Person** Rechnung tragen. Namentlich ist zu beachten, dass auch die Bekanntgabe (nur) von Name, Adresse oder Geburtsdatum je nach Zusammenhang zu einer Verletzung der Persönlichkeitsrechte führen kann. Das Bundesorgan hat demzufolge vor der Bekanntgabe die Pflicht, eine **Interessenabwägung** vorzunehmen. Es muss abklären, ob der Bekanntgabe wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person entgegenstehen. Darüber hinaus müssen selbstredend auch hier die allgemeinen datenschutzrechtlichen Grundsätze (Art. 4, 5 DSG) beachtet werden.

Insofern stellt Art. 19 Abs. 2 DSG **keine Grundlage für die freie und voraussetzungslose Bekanntgabe** dieser Daten dar; vielmehr ist jeweils im Einzelfall danach zu fragen, ob und inwieweit die Persönlichkeitsrechte der Betroffenen beeinträchtigt werden und den allgemeinen Grundsätzen im Falle einer Bekanntgabe Rechnung getragen wird.
So muss die Bekanntgabe allein auf der Grundlage von Art. 19 Abs. 2 DSG etwa dann verweigert werden, wenn schon der Umstand der Bekanntgabe der Stammdaten Aufschluss über darüber hinausgehende Angaben über die betreffende Person geben. So impliziert etwa allein die Tatsache, dass eine Strafverfolgungsbehörde des Bundes über die Stammdaten einer Person verfügt, dass diese Person möglicherweise eine wie auch immer geartete Rolle in einem Verfahren spielt (BBl 1988 II 471). Im Übrigen ist ganz allgemein zu beachten, dass auch Daten, die für sich genommen einen denkbar geringen Informationsgehalt haben (wie eben die Stammdaten), grundrechtserhebliche Auswirkungen auf die Persönlichkeitsrechte entfalten können, dies insbesondere angesichts bestehender Bearbeitungs- und Verknüpfungsmöglichkeiten.

Lösung Fall 13 (vgl. BGE 2A.424/2000):
Art. 19 Abs. 1 lit. a DSG sieht vor, dass Bundesorgane Personendaten bekannt geben dürfen, wenn die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind. Da es sich bei den Daten, welche über das Vorliegen einer Scheinehe Aufschluss geben können, um solche handelt, die zur Erfüllung der ausländerrechtlichen Aufgaben unentbehrlich sind, kann das Vorliegen dieser Voraussetzung bejaht werden. Fraglich könnte jedoch sein, ob dem Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG) entsprochen wurde. Jedoch betreffen sowohl das Asylrecht als auch das Ausländerrecht letztlich die Frage der Anwesenheitsberechtigung von Ausländern in der Schweiz. Die Daten werden demnach nicht zu einem Zweck verwendet, welcher mit dem Zweck der ursprünglichen Datenerhebung nicht vereinbar wäre, so dass im vorliegenden Fall Zweckidentität anzunehmen ist. Die Datenbekanntgabe durch das Bundesamt für Migration stand damit mit den gesetzlichen Vorgaben in Einklang; es lag weder ein Verstoss gegen Art. 19 DSG noch ein solcher gegen Art. 4 Abs. 3 DSG vor.

Lösung Fall 14:
Der Schweizerische Nationalfonds ist eine Stiftung, die mit der Förderung der Forschung und damit öffentlichen Aufgaben betraut ist und vom Bund finanziert wird, so dass er als Bundesorgan im Sinne des Art. 3 lit. h DSG anzusehen ist und somit dem DSG untersteht. Eine gesetzliche Grundlage für die Bekanntgabe der hier in Frage stehenden Personendaten (Verstoss gegen die Regeln wissenschaftlicher Redlichkeit bei der Gesuchseingabe durch eine bestimmte Person) ist nicht ersichtlich. Aber auch die Voraussetzungen des Art. 19 Abs. 1 lit. a DSG sind nicht erfüllt: Erstens sollen die Daten offenbar „spontan" weitergegeben werden, während diese Bestimmung zumindest grundsätzlich nur dann greifen kann, wenn ein entsprechender Antrag des Empfängers vorliegt. Zweitens soll die Bekanntgabe aber systematisch (nämlich bei jedem festgestellten Verstoss gegen die Regeln der wissenschaftlichen Redlichkeit zumindest durch an Hochschulen angestellte Personen) erfolgen, so dass es hier gerade nicht mehr um eine Bekanntgabe im Einzelfall geht. Hieran ändert auch der Umstand nichts, dass die Anzahl solcher Verstösse durchaus sehr gering sein dürfte.

2. Insbesondere: die Bekanntgabe im Rahmen der behördlichen Information der Öffentlichkeit

Fall 15:
Das Bundesamt für Verkehr erstellt in Zusammenarbeit mit einem privaten Auftragnehmer eine Studie über die Frage der „Machbarkeit" der Einführung des „Roadpricing" in der Schweiz. In der Studie werden sowohl rechtliche als auch technische Fragen erörtert. Die Studie soll der Vorbereitung entsprechender Gesetzgebungsentwürfe dienen bzw. deren Sachdienlichkeit eruieren.
X, ein politisch interessierter Bürger, verlangt auf der Grundlage des BGÖ Einblick in die (nicht veröffentlichten) Ergebnisse der Studie und möchte zudem die Namen der Verfasser kennen (sowohl die mit der Studie befassten Mitarbeiter des Bundesamtes für Verkehr als auch des privaten Auftragnehmers).
Muss seinem Gesuch entsprochen werden?

Fall 16 (vgl. Empfehlung des EDÖB, in EDÖB-Newsletter „datum" 1/2009):
Ein neuer Bundesrat trennt sich nach Amtsantritt von zwei hohen Angestellten seines Departements. In der Medienmitteilung heisst es lediglich, dass die Arbeitsverträge aufgelöst wurden, weil die gemeinsame Basis für eine erfolgreiche Zusammenarbeit nicht gegeben sei.
Ein Journalist will über dieses Ereignis eine Reportage schreiben und will es genauer wissen. Er verlangt die Kopien der Arbeitsverträge, die vom früheren Chef gewährten Spezialbedingungen sowie die beiden Auflösungsvereinbarungen. Das Departement ist der Ansicht, dass die Personendaten der beiden Auflösungsvereinbarungen nicht anonymisiert werden können. Darum verweigert es den Zugang aus Datenschutzgründen, namentlich zum Schutz der Persönlichkeit der beiden Funktionäre. Der Journalist ist damit nicht einverstanden und reicht beim EDÖB einen Schlichtungsantrag ein, Wie könnten die Empfehlungen des EDÖB lauten?

Art. 19 Abs. 1bis und Art. 19 Abs. 3bis DSG wurden im Gefolge des Erlasses des im Juli 2006 in Kraft getretenen Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) in das DSG aufgenommen. Diese Bestimmungen regeln die Bekanntgabe von Personendaten aus Gründen der **Transparenz und Öffentlichkeit der Verwaltung**.

Das **BGÖ** soll die **Transparenz der Tätigkeit der Bundesverwaltung** erhöhen und sieht insofern (auf Bundesebene) einen Wechsel von dem bis dahin geltenden Grundsatz der Geheimhaltung von bei der Verwaltung vorhandenen Informationen (mit Öffentlichkeitsvorbehalt) zum **Grundsatz der Öffentlichkeit der Verwaltung (mit Geheimhaltungsvorbehalt)** vor. Durch diese Einführung des Öffentlichkeitsprinzips in der Verwaltung drängte sich schon deshalb eine Koordination zwischen dem BGÖ und dem DSG auf, weil

die grundsätzlich öffentlichen Informationen selbstredend auch (grundsätzlich geschützte) Personendaten enthalten können. Die Regelung im BGÖ sieht diesbezüglich Folgendes vor:

- **Art. 7 Abs. 2 BGÖ** formuliert zwar den Grundsatz, dass der Zugang zu amtlichen Dokumenten entsprechend eingeschränkt wird, wenn hierdurch die Privatsphäre Dritter beeinträchtigt werden kann; eine Bekanntgabe ist aber gleichwohl möglich, wenn das **öffentliche Interesse am Zugang „ausnahmsweise" überwiegt.**
- **Art. 9 Abs. 1 BGÖ** verpflichtet die Behörden, amtliche Dokumente, die Personendaten enthalten, vor der Einsichtnahme nach Möglichkeit zu **anonymisieren**. Ist dies aber nicht möglich, sind Zugangsgesuche, die sich auf Dokumente beziehen, in denen Personendaten vorhanden sind, materiell nach **Art. 19 DSG** zu beurteilen (**Art. 9 Abs. 2 BGÖ**).

Damit wurde der Erlass einer Art **Koordinationsbestimmung im DSG** notwendig, was durch Art. 19 Abs. 1^{bis} und Art. 19 Abs. 3^{bis} DSG geschehen ist. Damit richtet sich die Bekanntgabe von Personendaten jedenfalls nach den Vorgaben des DSG, wobei für das **Zugangsverfahren** für Gesuche Einzelner das **BGÖ** einschlägig ist (Art. 9 Abs. 2 S. 2 BGÖ). Dieses Zugangsverfahren ist in Art. 10 ff. BGÖ geregelt. Im Übrigen können die von einer Bekanntgabe (möglicherweise) betroffenen Personen die ihnen nach **Art. 25 DSG** zustehenden Rechte (3. Kap. B.) im Rahmen des Verfahrens nach dem BGÖ geltend machen (**Art. 25^{bis} DSG**).
Bemerkenswert und für die Auslegung und Anwendung der für den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, massgeblich ist der Umstand, dass die erwähnten Bestimmungen des BGÖ und des DSG erkennen lassen, dass bei einem Konflikt zwischen dem Interesse der Öffentlichkeit am Zugang zu amtlichen Dokumenten und der dadurch (möglicherweise) implizierten Beeinträchtigung der Privatsphäre dem **Persönlichkeitsschutz grundsätzlich Vorrang** einzuräumen ist: Denn grundsätzlich sind Personendaten zu anonymisieren; falls dies nicht möglich ist, ist ihre Bekanntgabe unter Berufung auf den Grundsatz der Öffentlichkeit der Verwaltung nur dann erlaubt, wenn ein überwiegendes öffentliches Interesse besteht.

Gemäss **Art 19 Abs. 1^{bis} DSG** dürfen im Rahmen der behördlichen Information, der Öffentlichkeit vom Amtes wegen oder gestützt auf das BGÖ (Art. 9 Abs. 2 BGÖ) **Personendaten** auch **ohne gesetzliche Grundlage bekannt gegeben werden**, wenn

- die betreffenden Personendaten im Zusammenhang mit der **Erfüllung öffentlicher Aufgaben stehen** und
- an ihrer Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

Dabei müssen diese Voraussetzungen **kumulativ** erfüllt sein. Angesichts des Ausnahmecharakters der Bekanntgabe von Personendaten in diesem Rahmen, der sich aus dem grundsätzlichen Vorrang des Persönlichkeitsschutzes im Verhältnis zum Anliegen der Transparenz der Verwaltung ergibt, muss Art. 19 Abs. 1^{bis} DSG **restriktiv** ausgelegt werden, so dass insbesondere hohe Anforderungen an das überwiegende Interesse zu stellen sind. Weiter sind die **allgemeinen Datenschutzgrundsätze** zu beachten, wobei insbesondere die Grundsätze der Verhältnismässigkeit und der Zweckbindung von Bedeutung sind.
Art 19 Abs. 3^{bis} DSG sieht vor, dass diejenigen Informationen, die gestützt auf Art. 19 Abs. 1^{bis} DSG (oder aufgrund einer anderen Rechtsgrundlage) bekannt gegeben werden dürfen, auch im Internet veröffentlicht werden dürfen. Sobald das öffentliche Interesse an diesen Informationen jedoch nicht mehr besteht, sind die betreffenden Daten wieder zu entfernen.

Damit ist jedenfalls eine **Interessenabwägung im Einzelfall** erforderlich. Bei dieser ist die Art der Daten zu berücksichtigen: So dürfte im Falle besonders schützenswerter Daten oder bei Persönlichkeitsprofilen in der Regel das Interesse der Betroffenen an der Nichtbekanntgabe überwiegen. Auch ist zu berücksichtigen, ob die Daten freiwillig oder aufgrund einer gesetzlichen Pflicht übermittelt wurden (BBl 2003 2033). Weiter spielt es eine Rolle, ob die betroffene Person eine Person von öffentlichem Interesse ist und sich die Informationen auf die öffentlichen Tätigkeiten beziehen. Auf Seiten des öffentlichen Interesses sind etwa solche von grosser Bedeutung, die das Funktionieren der Institutionen betreffen (z.B. Verträge von Bundesorganen mit Privaten, insbesondere über grosse Summen, oder mögliche systematische Korruptionsfälle in der Verwaltung).

Bei der **aktiven Information** der Öffentlichkeit über Dokumente mit Personendaten sollten die Bundesbehörden angesichts des damit verbundenen Risikos für die Privatsphäre der Betroffenen – die zudem von der Veröffentlichung häufig keine vorgängige Kenntnis erlangen – grösste Zurückhaltung walten lassen. Dies gilt insbesondere für Informationen auf dem Internet: In aller Regel wird hier kein überwiegendes öffentliches Interesse gerade an dieser Publikationsform bestehen, sondern – sofern eine Veröffentlichung überhaupt durch ein überwiegendes öffentliches Interesse gerechtfertigt ist – die Veröffentlichung im Amtsblatt oder durch eine Einsichtsmöglichkeit vor Ort ausreichend sein.

Lösung Fall 15:
Soweit es bei dem Gesuch (lediglich) um den Inhalt der Studie selbst geht, ist davon auszugehen, dass diese keine persönlichen Daten enthält, so dass dieses Gesuch vollumfänglich auf der Grundlage des BGÖ zu bearbeiten ist.
Soweit es um die Namen der Verfasser geht, wird der Zugang zu Personendaten verlangt. Hieran ändert auch der Umstand nichts, dass es sich „nur" um die Namen handelt, denn allein der Umstand, dass eine bestimmte Person eine bestimmte Studie verfasst hat, stellt eine Angabe dar, die sich auf eine bestimmte Person bezieht (Art. 3 lit. a DSG). Das Zugangsbegehren ist demnach nach Art. 19 Abs. 1^{bis} DSG zu beurteilen:

- Die verlangten Personendaten stehen im Zusammenhang mit der Erfüllung öffentlicher Aufgaben (Art. 19 Abs. 1^{bis} lit. a DSG), denn es geht um die Verfasser einer Studie, die das Bundesamt für Verkehr im Rahmen seines Tätigkeitsfeldes zur Vorbereitung der Legislativtätigkeit erstellte bzw. erstellen liess.
- Fraglich könnte hingegen sein, ob ein überwiegendes öffentliches Interesse an der Bekanntgabe besteht. Insgesamt dürften die besseren Gründe für die Bejahung eines überwiegenden öffentlichen Interesse sprechen: Denn durch eine Bekanntgabe der in Frage stehenden Personendaten wird die Persönlichkeit der Betroffenen allenfalls marginal beeinträchtigt. Dies gilt insbesondere für die Mitarbeiter des Bundesamtes, die diese Aufgabe im Rahmen ihrer amtlichen Tätigkeit erfüllten. Aber auch der private Auftragnehmer dürfte bei solchen Fallgestaltungen in der Regel nicht schwerwiegend in seinen Persönlichkeitsrechten betroffen sein. Weiter ist zu beachten, dass es hier um Arbeiten geht, die die Legislativtätigkeit vorbereiten. Die Transparenz dieser Vorgänge entfaltet unmittelbar Auswirkungen auf die Transparenz des Legislativprozesses insgesamt, so dass ein eher gewichtiges öffentliches Interesse an der Bekanntgabe nicht nur des Inhalts der Studie, sondern auch der beteiligten Akteure besteht, können diese doch durchaus von Interesse sein.

Lösung Fall 16 (vgl. Empfehlung des EDÖB, in EDÖB-Newsletter „datum" 1/2009):
Auf der Grundlage des BGÖ kann nur zu Dokumenten Zugang verlangt werden, die nach des Inkrafttreten des Öffentlichkeitsgesetzes, also nach dem 1. Juli 2006, erstellt oder einer Bundesbehörde mitgeteilt worden sind.
Da die beiden Arbeitsverträge sowie die gewährten Spezialbedingungen älteren Datums sind, muss das Departement sie nicht zugänglich machen.
Anders verhält es sich mit den Auflösungsvereinbarungen, diese wurden zu einem späteren Zeitpunkt erstellt. Sie enthalten die Namen der Betroffenen und regeln Sachverhalte, die ihre Persönlichkeit betreffen, so dass Personendaten im Sinne des Datenschutzgesetzes vorliegen. In diesem Falle treffen Öffentlichkeitsprinzip und Datenschutz aufeinander. Art. 9 BGÖ sieht für eine solche Fallgestaltung ein Vorgehen in zwei Stufen vor:

- Die Bundesbehörde muss die Daten der Drittpersonen anonymisieren, bevor das Dokument dem Gesuchsteller zugänglich gemacht wird.
- Können die Personendaten nicht anonymisiert werden, muss sich die Behörde für die Bekanntgabe der Daten nach dem Datenschutzgesetz (Art. 19 DSG) richten. Diesem zufolge darf die Bekanntgabe nur erfolgen, wenn sie ausdrücklich in einer gesetzlichen Grundlage vorgesehen ist oder die betroffene Person vorgängig bereits ihre Zustimmung dafür gegeben hat. Ausnahmsweise können Personendaten auch bekannt gegeben werden, wenn dafür ein überwiegendes öffentliches Interesse besteht.

Im vorliegenden Fall ist damit zu prüfen, ob das Interesse der Öffentlichkeit am Zugang überwiegt (die Anonymisierung war nicht möglich). Es ist also m.a.W. zwischen dem öffentlichen Interesse am Zugang zu den Auflösungsvereinbarungen und dem privaten Interesse der betroffenen Drittpersonen am Schutz ihrer Privatsphäre abzuwägen. Der EDÖB kam zum Schluss, dass das Interesse der Öffentlichkeit am Zugang zu den Auflösungsvereinbarungen das Interesse der beiden Betroffenen am Schutz ihrer Privatsphäre überwiegt. Hierfür spricht insbesondere auch der Umstand, dass es um die Frage der ordnungsgemässen Verwaltung bzw. ihres Funktionierens geht. Er empfahl daher dem Departement, dem Journalisten Kopien der Auflösungsvereinbarungen zuzustellen.

3. Zusätzliche Vorgaben für die Bekanntgabe (Art. 19 Abs. 4 DSG)$

Eine grundsätzlich nach Art. 19 DSG zulässige Datenbekanntgabe hat gemäss Art. **19 Abs. 4 DSG** gleichwohl zu **unterbleiben**, wenn:

- wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person oder
- gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.
- Damit ist vor einer an sich zulässigen Bekanntgabe immer zunächst noch zu prüfen, ob einer der genannten Einschränkungsgründe einer Bekanntgabe entgegensteht. Allerdings kommt dieser „Vorbehalt" immer dann nicht zum Zuge, wenn eine **gesetzliche Grundlage** die Bekanntgabe und den Umfang der Bekanntgabe der Personendaten **abschliessend** regelt. Insofern sind parallele Grundsätze wie diejenigen in Bezug auf die Massgeblichkeit der allgemeinen datenschutzrechtlichen Grundsätze bei der Anwendung spezialgesetzlicher Grundlagen anzuwenden (2. Kap. C.II.1.).

Die Frage, ob eine bestimmte **spezialgesetzliche Regel** tatsächlich auch in Bezug auf die in Art. 19 Abs. 4 DSG genannten Einschränkungsgründe **abschliessend** ausgestaltet ist, kann aber mitunter schwierig zu beantworten sein. Jedenfalls dürfte eine in jeder Hinsicht abschliessende Regelung immer dann zu verneinen sein, wenn die einschlägige gesetzliche Grundlage keine Verpflichtung zur Datenbekanntgabe, sondern lediglich eine Ermächtigung, vorsieht. Angesichts der grundsätzlichen Bedeutung der durch Art. 19 Abs. 4 DSG vorgesehenen Interessenabwägung ist es aber auch denkbar, dass bei einer Verpflichtung zur Bekanntgabe zumindest in Bezug auf Teilaspekte des Art. 19 Abs. 4 DSG die Abgeschlossenheit der jeweiligen Regelung zu verneinen ist.

Wesentliche **öffentliche Interessen** sind etwa solche der militärischen Sicherheit, des Staatsschutzes und des Polizeiwesens. Ein offensichtlich **schutzwürdiges Interesse einer betroffenen Person** kann beispielsweise das Bedürfnis an der Geheimhaltung einer Identität sein, wenn eine Person in eine gerichtliche Untersuchung einbezogen ist. Deutlich wird damit auch, dass sich dieser Einschränkungsgrund zumindest teilweise mit den ggf. sowieso anzuwendenden allgemeinen datenschutzrechtlichen Grundsätzen überschneidet. Im Falle des Vorliegens eines solchen öffentlichen oder privaten Interesses ist die angefragte Stelle grundsätzlich verpflichtet, eine Interessenabwägung zwischen der ermächtigenden gesetzlichen Grundlage und den betroffenen Interessen vorzunehmen (VPB 62.58 E.3.c).
Aus dem Vorbehalt der **gesetzlichen Geheimhaltungspflichten und besonderen Datenschutzvorschriften** folgt nicht in allen Konstellationen zwingend, dass die Geheimhaltungspflicht bzw. die besondere Datenschutzvorschrift einer Datenbekanntgabe immer vorgehen: In BGE 124 III 170 E. 4b hatte sich die Sozialversicherungsanstalt des Kantons Zürich, gestützt auf Art. 19 Abs. 4 lit. b DSG, vergeblich versucht zu wehren, Personendaten an das Betreibungsamt bekannt zugeben, welches im Rahmen eines Pfändungsvollzugs die Bekanntgabe der Höhe der Leistungen an einen Schuldner sowie des Lohnes der Ehefrau verlangte. Das Bundesgericht hielt fest, dass die Auskunft nicht unter Berufung auf die Schweigepflicht verweigert werden könne, wenn der Schuldner selbst zur Auskunft gegenüber dem Betreibungsamt verpflichtet sei.

IV. Spezifische Bearbeitungsformen (Art. 21, 22 DSG)

1. Angebot von Unterlagen an das Bundesarchiv (Art. 21 DSG)

Personendaten die nicht mehr ständig benötigt werden, müssen dem **Bundesarchiv angeboten** werden (**Art. 21 Abs. 1 DSG**).

Diese Pflicht ist vor dem Hintergrund des Art. 6 des **Archivierungsgesetzes** vom 26. Juni 1998 zu sehen, der eine allgemeine Anbietepflicht für Bundesorgane einführt. Es ist allerdings zweifelhaft, ob diese letztlich

„allumfassende“ Pflicht in der Praxis angesichts der Unmenge von Dokumenten, insbesondere auf elektronischen Datenträgern, die in der Verwaltung anfallen, praktikabel ist.

In der Regel ist davon auszugehen, dass **mit dem Wegfall des Bearbeitungszwecks**, **Personendaten nicht mehr benötigt** werden. Beim Bestehen einer **gesetzlichen Aufbewahrungsdauer** können die Vernichtung respektive die Archivierung grundsätzlich erst nach deren Ablauf erfolgen.
Nach Art. 21 Abs. 2 DSG haben die Bundesorgane die Personendaten welche vom Bundesarchiv als **„nicht archivwürdig“** bezeichnet werden, zu **vernichten** (ausser wenn diese anonymisiert sind oder zu Beweis- oder Sicherheitszwecken aufbewahrt werden müssen), eine Pflicht, die letztlich den **Verhältnismässigkeitsgrundsatz** konkretisiert (müssen doch nicht mehr benötigte Personendaten grundsätzlich vernichtet werden, da der mit dem Aufbewahren der Daten implizierte Eingriff in die Persönlichkeitsrechte nicht mehr notwendig ist).

Problematisch ist die Frage der Zulässigkeit der Aufbewahrung von Personendaten insbesondere im Rahmen der polizeilichen Tätigkeit, etwa, wenn es um Unterlagen über ein abgeschlossenes oder eingestelltes Strafverfahren geht. Das Bundesgericht geht hier davon aus, dass die Aufbewahrung von Akten und damit erkennungsdienstlichem Material über eine abgeschlossene Untersuchung grundsätzlich schon deshalb möglich sein muss, weil Personen, die sich ein strafrechtliches Delikt einer gewissen Schwere haben zuschulden kommen lassen, auch in Zukunft möglicherweise Straftaten begehen könnten und die aufbewahrten Akten zu deren Aufklärung beitragen könnten (BGE 120 Ia 147). Diese Rechtsprechung sollte jedoch nicht verallgemeinert werden, sondern es sollte in jedem Einzelfall die Verhältnismässigkeit der Aufbewahrung überprüft werden, insbesondere im Falle von Freisprüchen oder möglicher Verletzungen der Unschuldsvermutung. Ganz allgemein ist zu beachten, dass sich die Persönlichkeit und das Verhalten von Individuen weiterentwickeln können und eine solche Datenaufbewahrung eine gewisse Stigmatisierungsgefahr – die durchaus auch Einfluss auf künftige Verfahren haben kann – entfalten kann. Jedenfalls ist aber zu beachten, dass gerade im Bereich der Polizei- und Justizbehörden in der Regel gesetzliche Aufbewahrungsfristen bestehen.

2. Bearbeiten von Personendaten für Forschung, Planung und Statistik (Art. 22 DSG)

Art. 22 DSG enthält eine **spezifische gesetzliche Grundlage** für **die Bearbeitung von Personendaten für nicht personenbezogene Zwecke** (insbesondere für Forschung, Planung und Statistik) durch Bundesorgane. Eine solche Bearbeitung ist unter drei kumulativ zu verstehenden Voraussetzungen zulässig (**Art. 22 Abs. 1 lit. a-c DSG**):

- Die Daten werden **anonymisiert**, sobald es der Zweck erlaubt.
- Der Empfänger gibt die Daten nur mit Zustimmung des Bundesorgans weiter.
- Die Ergebnisse werden so veröffentlicht, dass die **betroffene Person nicht bestimmbar** ist.

Sind diese drei Voraussetzungen kumulativ erfüllt, ist das Bundesorgan von der Einhaltung der Zweckbindung (Art. 4 Abs. 3 DSG), dem Bestehen einer Rechtsgrundlage im Sinne von Art. 17 Abs. 2 DSG und von der Einhaltung des Art. 19 Abs. 1 DSG entbunden (Art. 22 Abs. 2 DSG).

Im Zusammenhang mit diesem Artikel ist insbesondere das **Bundesstatistikgesetz** von Bedeutung; es ergänzt und konkretisiert Art. 22 DSG (siehe u.a. Art. 4 BStatG, Grundsätze der Datenbeschaffung, und Art. 15 BStatG, Datensicherheit und Datenaufbewahrung).
Weiter wird Art. 22 DSG für den Bereich der medizinischen Forschung durch Art. 32 DSG und Art. 321bis StGB ergänzt.

3. Kapitel Rechte Einzelner

Literatur: Maurer-Lambrou/Vogt-MAURER-LAMBROU, Art. 8 DSG; Maurer-Lambrou/Vogt-GRAMINGA, Art. 9 DSG; Maurer-Lambrou/Vogt-BANGERT, Art. 25 DSG; EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz; EDÖB, Leitfaden über die Rechte der betroffenen Person bei der Bearbeitung von Daten; EDÖB-Newsletter „datum"; Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988; 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 der Menschen bei der automatischen Verarbeitung von Personendaten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung vom 19. Februar 2003; EDÖB, Kommentar zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG).

Da die Bearbeitung von Personendaten in die Persönlichkeitsrechte Einzelner eingreift, bedarf es für einen wirksamen Schutz dieser Rechte der Einzelnen nicht nur die Einhaltung der bis jetzt erörterten materiell-rechtlichen Vorgaben, sondern den Einzelnen sind auch diejenigen Rechte einzuräumen, die es ihnen **ermöglichen, ihre Rechte bzw. die Einhaltung der gesetzlichen Vorgaben durchzusetzen**. Vor diesem Hintergrund verankert das DSG eine ganze Reihe von Rechten Einzelner, wobei zwischen dem Auskunftsrecht (A.) und sonstigen Ansprüchen (B.) unterschieden werden kann.

Daneben stellt selbstredend auch das Recht auf Information ein solches Recht Einzelner dar, das jedoch bereits im Zusammenhang mit der Rechtmässigkeit der Datenbearbeitung als solche eine Rolle spielt und im Zusammenhang mit dem Grundsatz der Transparenz (2. Kap. A.VI.) erörtert wurde.

A Auskunftsrecht

Fall 17 (vgl. BGE 125 II 225):
M und G wurden im April 1995 in Sarajevo verschleppt. Aufgrund der Bemühungen des Eidgenössischen Departements für auswärtige Angelegenheiten erfolgte im Mai 1995 die Freilassung der Verschleppten. M und G ersuchten später gestützt auf das DSG beim EDA um Auskunft und Einsicht der Akten. Dem Ersuchen wurde teils stattgegeben, teils wurde es mit förmlicher Verfügung abgewiesen. Welches könnten die Gründe sein, weshalb das EDA dem Auskunftsersuchen (Art. 8 DSG) nur teilweise entsprochen hat und wo findet sich die passende Rechtsgrundlage?

Art. 8 DSG – der in den allgemeinen Datenschutzbestimmungen figuriert – räumt **jeder urteilsfähigen Person**, unabhängig von Alter, Wohnsitz und Nationalität, das Recht ein, Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen. Der Nachweis eines irgendwie gearteten Interesses ist nicht erforderlich.

Das Auskunftsrecht ist ein **zentrales Element des Datenschutzes** und eine **Grundvoraussetzung** für die Überprüfung der Einhaltung der Datenschutzgesetzgebung und der Ausübung der Kontrollrechte. Es ist von herausragender Bedeutung, denn nur wenn eine betroffene Person erfahren kann, wer über sie Daten bearbeitet, ist sie in der Lage gegen eine allfällige unzulässige Datenbearbeitung vorzugehen.

Das Auskunftsrecht ist ein jeder Person voraussetzungslos zustehendes **höchstpersönliches Recht** und kann nicht für Dritte ausgeübt werden. Es ist nicht übertragbar und nicht vererblich (s. aber Art. 1 Abs. 7 VDSG) sowie keiner zeitlichen Befristung unterworfen (VPB 62.38). Auf das Auskunftsrecht kann im Voraus nicht verzichtet werden (Art. 8 Abs. 5 DSG). Eine entsprechende Verzichtserklärung ist nichtig.

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; kein Interessennachweis ist für nahe Verwandte und Ehepartner nötig, bei denen durch das Gesetz das Vorliegen eines Interesses vermutet wird.

Adressat des Auskunftsrechts ist grundsätzlich der **Inhaber der Datensammlung**. Dies gilt auch, wenn er die Datensammlung durch einen Dritten bearbeiten lässt (Art. 10a DSG),

wobei den Dritten unter den Voraussetzungen von Art. 8 Abs. 4 DSG auch eine Auskunftspflicht treffen kann.

Hat eine Datensammlung **mehrere Inhaber**, ist jeder zur Auskunft verpflichtet, es sei denn, es bestehe eine klare interne Rollenverteilung (**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).

Gegenstand des Auskunftsrechts sind Daten einer Datensammlung, die sich auf die eigene Person beziehen. Die **betroffenen Personen** können nach Art. 8 Abs. 2 DSG **Auskunft verlangen**

- über alle zu ihrer Person in einer **Datensammlung vorhandenen Daten**, einschliesslich der Angaben, woher sie stammen;
- über den **Zweck der Bearbeitung** und gegebenenfalls die Rechtsgrundlagen des Bearbeitens;
- über die Kategorien der **bearbeiteten Daten**;
- über die Kategorien der **Beteiligten** an einer Datensammlung und
- über die Kategorien der Personen und Stellen, an die die Daten übermittelt werden (**Datenempfänger**).

Gemäss Art. 1 Abs. 1 VDSG muss der **Auskunftsantrag** in der Regel **schriftlich** verfasst sein, und die gesuchstellende Person muss sich über ihre Identität ausweisen. Grundsätzlich können Auskunftsbegehren und Auskunftserteilung auch auf elektronischem Weg erfolgen, sofern die Identifizierung der antragstellenden Person sowie die Sicherheit der Daten gewährleistet ist (Art. 1 Abs. 2 VDSG), wobei ausnahmsweise mit dem Einverständnis des Inhabers der Datensammlung oder auf dessen Vorschlag hin die betroffene Person ihre Daten an Ort und Stelle einsehen kann (Art. 1 Abs. 3 VDSG). Ein Einsehen vor Ort kommt aber nur in Betracht, wenn der Antragsteller einverstanden ist (BGE 125 II 321). Auch eine mündliche Auskunft ist möglich, wenn die betroffene Person eingewilligt hat (Art. 1 Abs. 3 VDSG).

Die **Auskunft** oder der begründete Entscheid über die Beschränkung des Auskunftsrechts muss **innert 30 Tagen**, seit dem Eingang des Auskunftsbegehrens erteilt werden. Mindestens muss der Inhaber der Datensammlung die Frist mitteilen, in der die Auskunft erfolgen wird (Art. 1 Abs. 4 VDSG).

Die Auskunft hat **in der Regel kostenlos** zu erfolgen (Art. 8 Abs. 5 DSG). Eine Kostenbeteiligung in Höhe von maximal 300 CHF kann nach Art. 2 VDSG ausnahmsweise verlangt werden;

- wenn die betroffene Person in den letzten zwölf Monaten die gewünschten Auskünfte bereits erhalten hat. 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.
- wenn die Auskunftserteilung einen besonders grossen Arbeitsaufwand verursacht, beispielsweise wenn langwierige Nachforschungen notwendig sind.

Auf Verlangen des Gesuchstellers muss eine Kostenbeteiligung in Form einer selbständig anfechtbaren Zwischenverfügung festgesetzt werden. Die Erhebung einer Kostenbeteiligung setzt, vorbehältlich eines ausserordentlich grossen Aktenumfanges, einen über das blosse Kopieren und Versenden der Akten hinausgehenden Aufwand voraus (vgl. VPB 65.50). Die Erhebung einer Kostenbeteiligung ist nicht zulässig, wenn der Gesuchsteller die Voraussetzungen der unentgeltlichen Rechtspflege erfüllt (vgl. VPB 65.49).

Das **Recht auf Auskunft** ist jedoch auch in **Art. 9, 10 DSG** abschliessend aufgeführten **Schranken** unterworfen, wobei diese Bestimmungen vor dem Hintergrund zu sehen sind, dass das **Auskunftsrecht die Regel** ist, während die **Einschränkung eine Ausnahme** darstellt. Im Zusammenhang mit den Tätigkeiten von Bundesorganen sind in erster Linie folgende Möglichkeiten der Verweigerung oder Einschränkung der Auskunft von Bedeutung:

- Ein **Gesetz im formellen** Sinn sieht eine solche Einschränkung vor (Art. 9 Abs. 1 lit. a DSG);
- Eine Verweigerung oder Einschränkung ist wegen **überwiegenden Interessen Dritter** erforderlich (Art. 9 Abs. 1 lit. b DSG);
- Es bestehen **überwiegende öffentlichen Interessen**, insbesondere der inneren oder äusseren Sicherheit der Schweiz, und die Einschränkung oder Verweigerung des Auskunftsrechts ist zu ihrer Wahrung erforderlich (Art. 9 Abs. 2 lit. a DSG);
- Die Auskunft oder die Information stellte den **Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens** in Frage (Art. 9 Abs. 1 lit. b DSG).

Nicht jedes **öffentliche Interesse** hat als überwiegend im Sinne von Art. 9 Abs. 2 DSG zu gelten. Rein verwaltungsinterne Anliegen (z.B. Effizienz der Verwaltungsabläufe oder der mit der Einsicht verbundene Aufwand bzw. die Kosten) oder politische Interessen (z.B. das Interesse eines Magistraten an seinem „guten Ruf" oder das Interesse an der möglichst raschen Beendigung des Gesetzgebungsverfahrens) begründen kein überwiegendes öffentliches Interesse. Der Verweigerungsgrund des überwiegenden öffentlichen Interesses i.S.v. Art. 9 Abs. 2 lit. a DSG kann nicht pauschal für bestimmte Kategorien von Auskunftsersuchen geltend gemacht werden, sondern muss im Einzelfall in Bezug auf diejenigen Aktenstücke, in die die Einsicht verweigert werden soll, konkret geprüft werden.
Im Übrigen ist gestützt auf Art. 9 Abs. 2 lit. b DSG eine Einschränkung des Auskunftsrechts nicht schon dann zulässig, wenn bloss die ferne Möglichkeit der **Infragestellung des Untersuchungszwecks** besteht, sondern nur, wenn diese Möglichkeit sich mit einiger Wahrscheinlichkeit aufdrängt.
Geht es um die Einschränkung des Auskunftsrechts aufgrund überwiegender Interessen Dritter oder aufgrund überwiegender öffentlicher Interessen, ist die **Güterabwägung** zwischen den Interessen des Gesuchstellers und den Interessen des Dritten bzw. den öffentlichen Interessen besonders wichtig, ist deren Ergebnis doch für die (Nicht-) Gewährung des Einsichtsrechts entscheidend, wobei jeweils zu beachten ist, 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 Dritter zu gewährleisten (vgl. VPB 62.55).

Der Inhaber der Datensammlung ist verpflichtet anzugeben, **aufgrund welcher gesetzlichen Bestimmung** und **aufgrund welcher Tatsachen** er die **Auskunft verweigert**, einschränkt oder aufschiebt (Art. 9 Abs. 4 DSG).

Lösung Fall 17 (vgl. BGE 125 II 225):
Der grundsätzliche Anspruch der Betroffenen auf Auskunft (Art. 8 DSG) kann nach Art. 9 Abs. 1 lit. b und Abs. 2 lit. a DSG wegen überwiegender Interessen Dritter oder wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, verweigert oder eingeschränkt werden. Der verantwortlichen Behörde ist ein gewisser Beurteilungsspielraum zuzugestehen. Das gilt insbesondere für den spezifischen Bereich der Diplomatie. Es gehört zu den überwiegenden öffentlichen Interessen und zum Schutz der inneren und äusseren Sicherheit der Schweiz, im Sinne von Art. 9 Abs. 2 lit. a DSG, das Funktionieren diplomatischer Kontakte sicherzustellen und den diplomatischen Handlungsspielraum in Krisensituationen aufrecht zu erhalten, so dass die teilweise Auskunftsverweigerung wohl aus diesen Gründen erfolgte.

B Sonstige Ansprüche

Fall 18 (vgl. VPB 68.69):
In der einschlägigen gesetzlichen Grundlage ist vorgesehen, dass die sog. Fahrzeughalterdaten (Name, Vorname und Adresse eines Fahrzeughalters) in Verbindung mit der Immatrikulationsnummer des Fahrzeugs veröffentlicht werden können (nicht müssen). Die zuständige Behörde veröffentlichte diese Angaben auf dem Internet. Fahrzeughalter A beantragt die Sperrung der Bekanntgabe seiner Daten mit der Begründung, er wolle es vermeiden, dass jeder wissen kann, welches Fahrzeug er fahre bzw. in Verbindung mit der Immatrikulationsnummer ihn als Fahrzeughalter seines Fahrzeugs identifizieren kann. Ist dem Antrag auf Sperrung stattzugeben?

Fall 19 (vgl. VPB 67.73):
Herr A stellt beim Bundesamt für Migration ein Gesuch um Berichtigung seiner Personendaten (die Angabe des Geburtsjahres soll von 1976 auf 1974 geändert werden). Das Bundesamt ist sich unschlüssig, wie es mit dieser Eingabe umgehen soll: Denn der Gesuchsteller selbst hat während des Asylverfahrens sein Geburtsjahr zweimal mit 1976 abgegeben und bestätigt; weitere Beweise wurden während des Verfahrens nicht vorgelegt. Mit der erwähnten Eingabe aber legt A neu einen Geburtsschein (mit dem Geburtsjahr 1974) vor; dieser ist jedoch ohne Foto und auch sonst hat das Amt Zweifel an der Glaubwürdigkeit dieser Urkunde. Wie muss das Bundesamt für Migration vorgehen?

Art. 5 Abs. 2, 20, 25 DSG sind eine Reihe von Ansprüchen der Betroffenen bzw. der Personen, die ein schutzwürdiges Interesse haben oder glaubhaft machen, gegen den Inhaber der Datensammlungen zu entnehmen, die sich teilweise wiederholen oder „ähnliche“ Rechte betreffen.

So wird das **Recht auf Berichtigung** 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, 25 DSG).
In Bezug auf den systematischen Zusammenhang dieser verschiedenen, die Rechte Einzelner betreffenden Bestimmungen, kann Folgendes festgehalten werden:

- 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 lit. a DSG** nochmals für Bundesorgane wiederholt wird. Für Bundesorgane ist die letztgenannte Vorschrift als spezifische Bestimmung massgeblich, wobei die rechtliche Tragweite beider Bestimmungen aber deckungsgleich sein dürfte.

- Die **Sperrung der Bekanntgabe rechtmässig bearbeiteter Daten** richtet sich nach **Art. 20 DSG**: Diese Bestimmung gewährt ein Abwehrrecht gegen die Bekanntgabe von Personendaten durch das verantwortliche Bundesorgan auch in denjenigen Fällen, in denen die Bekanntgabe grundsätzlich zulässig ist bzw. wäre. Hingegen bezieht sich **Art. 25 Abs. 3 DSG** auf die **Sperrung der Bekanntgabe im Falle der widerrechtlichen Bearbeitung** und damit auch der widerrechtlichen Bekanntgabe von Personendaten. 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.

Im Einzelnen können folgende Rechte bzw. Ansprüche unterschieden werden: Recht auf Berichtigung (I.), Recht auf Sperrung der Bekanntgabe an Dritte (II.), „Bekanntmachungsansprüche“ (III.) sowie die sonstigen im Zuge einer widerrechtlichen Bearbeitung entstehenden Ansprüche (IV.).

I. Berichtigung

Art. 5 Abs. 2, Art. 25 Abs. 3 lit. a DSG enthalten einen Anspruch der durch unrichtige Daten betroffenen Person, wonach diese die **Berichtigung von unrichtigen Daten** verlangen kann.

Dieser Anspruch auf Berichtigung ergibt sich folgerichtig aus dem Grundsatz der Datenqualität (Art. 5 DSG, 2. Kap. A.VII.), denn das datenbearbeitende Organ hat sich über die **Richtigkeit der Daten** zu vergewissern und muss diese korrigieren oder vernichten, wenn sie im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Deutlich wird damit auch, dass die Bundesorgane nicht nur im

Falle der Geltendmachung des Anspruchs auf Berichtigung zur Korrektur verpflichtet sind, sondern dass dies auch eine **objektiv-rechtliche Pflicht** darstellt. Die Richtigkeit von Personendaten ist demnach von Amts wegen zu prüfen, so dass – sobald konkrete Anhaltspunkte für die Unrichtigkeit von Daten bestehen (aufgrund der Geltendmachung eines Berichtigungsanspruchs oder aus sonstigen Gründen) – eine **entsprechende Prüf- und ggf. Berichtigungspflicht** ausgelöst wird. Kommt das verantwortliche Bundesorgan dieser Pflicht nicht oder nur ungenügend nach, so wird die **zukünftige Bearbeitung der betreffenden Daten „automatisch" widerrechtlich**, und begründet somit einen Unterlassungs- und Berichtigungsanspruch gemäss Art. 25 Abs. 1 lit. a DSG (3. Kap. B.IV.).

Die Geltendmachung des Rechts auf Berichtigung durch den Betroffenen ist regelmässig erst nach Kenntnisnahme der Unrichtigkeit denkbar. Das Berichtigungsrecht ist deshalb im Zusammenhang mit dem **Auskunftsrecht (Art. 8 DSG)** zu sehen (3. Kap. A.).
Voraussetzung für die Begründetheit des Berichtigungsanspruchs sind einzig die Unrichtigkeit der bisher bearbeiteten Daten und die Richtigkeit derjenigen, die gemäss dem Antrag des Gesuchstellers die unrichtigen Daten ersetzen soll.

Der Anspruch auf Berichtigung knüpft damit an die **Existenz falscher bzw. unrichtiger Daten** an. Er kann daher etwa nicht geltend gemacht werden, wenn keine offensichtlich unrichtigen Sachverhaltsdarstellungen vorgeworfen werden können (nicht publizierter BGE vom 2. Mai 2001, 1A.6/2001). Zum Begriff der Richtigkeit bereits 2. Kap. A.VII.1.

Jede noch so nebensächliche Unrichtigkeit ist zu berichtigen. Der Datenbearbeiter kann weder einen Rechtfertigungsgrund geltend machen, noch das schutzwürdige Interesse der betroffnen Person bestreiten bzw. ein eigenes überwiegendes Interesse anführen. Daraus folgt, dass der Berichtigungsanspruch ausnahmslos und uneingeschränkt besteht. 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 Realität** gebracht werden. Grundsätzlich kommen verschiedene Arten von Berichtigungen in Frage, z.B. eine Veränderung durch inhaltliche 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 (nicht publizierter BGE vom 29. März 2006, 1A.295/2005), ist durch den Datenbearbeiter innerhalb einer **angemessenen Frist** vorzunehmen. Eine 30-tägige Frist wird sich im Regelfall analog zum Auskunftsrecht als angemessen erweisen.

II. Sperrung der Bekanntgabe

Die betroffene Person bzw. diejenige Person mit einem schutzwürdigen Interesse kann aufgrund von Art. 20 DSG (1.) oder aufgrund von Art. 25 Abs. 1, Abs. 3 lit. a DSG (2.) verlangen, dass das betreffende Bundesorgan die Bekanntgabe bestimmter Personendaten sperrt.

1. Art. 20 DSG

Gemäss **Art. 20 DSG** kann eine Person, die ein schutzwürdiges Interesse glaubhaft macht, vom verantwortlichen Bundesorgan die Sperrung der Bekanntgabe bestimmter Personendaten verlangen. Wie bereits erwähnt (3. Kap. B., am Anfang), kommt Art. 20 DSG nur unter der Voraussetzung zur Anwendung, dass die **Bekanntgabe** der betreffenden Daten in Anwendung der Vorgaben des Art. 19 DSG (2. Kap. C.III.) an sich **rechtmässig** wäre.

Im Falle der Nichterfüllung der Voraussetzungen des Art. 19 DSG ist die Datenbekanntgabe schon aus diesem Grund rechtswidrig und jedenfalls zu unterlassen; ein entsprechender Anspruch – der auch in

sonstigen Fällen der widerrechtlichen Bearbeitung zum Zuge kommt – ist in Art. 25 Abs. 1, Abs. 3 lit. a DSG verankert (3. Kap. B.II.2.).
Wird eine nach Art. 20 DSG verlangte Sperrung missachtet und erfolgt – obwohl kein Grund für die Aufhebung der Datensperre gegeben war – eine Datenbekanntgabe, so ist diese Datenbearbeitung widerrechtlich mit der Folge, dass die Ansprüche nach Art. 25 DSG greifen.
Art. 20 DSG kommt nur in Bezug auf die **Bekanntgabe von Daten** zum Zuge, nicht aber bei anderen Bearbeitungsvorgängen. In Bezug auf diese stehen lediglich die sich aus Art. 25 DSG ergebenden Ansprüche zur Verfügung, die allerdings eine widerrechtliche Bearbeitung voraussetzen (3. Kap. B.II.2.).

Der Hintergrund des Rechts auf Sperrung der Bekanntgabe ist darin zu sehen, dass jede **Person grundsätzlich über ihre Daten verfügen** kann, wie es ihr beliebt, so dass sie dementsprechend auch grundsätzlich jede Bekanntgabe ihrer Daten verhindern können muss.
Allerdings ist Art. 20 DSG **kein „absolutes" Recht auf Sperrung der Bekanntgabe** zu entnehmen: Vielmehr verweigert das Bundesorgan die Sperrung (oder hebt sie nachträglich auf), wenn eine **Rechtspflicht zur Bekanntgabe** besteht (eine solche kann auf einer gesetzlichen Grundlage – selbst auf Verordnungsebene – beruhen), oder wenn die Sperrung der Bekanntgabe die **Erfüllung der gesetzlichen Aufgabe** des Bundesorgans gefährdet. Diesem Ausnahmegrund dürfte bei Bekanntgaben zwischen Behörden eine wichtige Rolle zukommen. Weiter bleibt das Öffentlichkeitsgesetz vorbehalten (Art. 20 Abs. 3 i.V.m. Art. 19Abs. 1^{bis} DSG).

Die entsprechende Entscheidung ist als Verfügung im Sinne von Art. 5 VwVG zu erlassen.
Anspruchsberechtigt ist jede **betroffene Person**, die ein **schutzwürdiges Interesse** glaubhaft macht:

- **Betroffen** ist eine Person, wenn eine gewisse Wahrscheinlichkeit besteht, dass das verantwortliche Bundesorgan ihre Daten an Dritte weitergibt (etwa, weil eine solche Bekanntgabe regelmässig erfolgt, oder weil das verantwortliche Organ im Einzelfall Daten bekannt geben will). Die Weitergabe muss noch nicht stattgefunden haben.

- Die Frage, ob ein **schutzwürdiges Interesse** vorliegt, ist in Anknüpfung an das Schutzgut des Art. 20 DSG, nämlich der Schutz der Einzelnen vor einer unkontrollierbaren Weitergabe ihrer Daten, zu bestimmen, so dass ein solches immer schon dann vorliegen dürfte, wenn der Einzelne glaubhaft macht, in seinen Persönlichkeitsrechten durch die Bekanntgabe betroffen zu sein, wobei eine solche Beeinträchtigung plausibel sein muss. Das Bundesorgan muss aber nicht selbst vom Vorliegen solcher Interessen überzeugt sein, so dass die Frage, welche Beeinträchtigungen als relevant anzusehen sind, grundsätzlich – unter dem Vorbehalt der erwähnten Plausibilität – durch den Betroffenen zu bestimmen ist. Insofern sind also an das Vorliegen eines schutzwürdigen Interesses keine allzu hohen Anforderungen zu stellen.

Die Ausübung von datenschutzrechtlichen Abwehrrechten (Widerspruchsrecht, Art. 12 Abs. 2 DSG und Sperrrecht Art. 20 DSG) ist grundsätzlich **kostenlos**. Für die Erhebung von Kosten bedarf es einer gesetzlichen Grundlage (vgl. VPB 64.73).
Das **Sperrrecht** kann **gegenüber jedem Empfänger von Daten** geltend gemacht werden. Die betroffene Person muss sich an das zuständige Organ wenden und die Daten, welche gesperrt werden sollen, genau bezeichnen. Das Sperrrecht kann nicht pauschal geltend gemacht werden. (BBl 1988 II 472).

2. Art. 25 DSG

Art. 25 Abs. 1, Abs. 3 lit. a DSG sieht ebenfalls einen **Anspruch auf Sperrung der Bekanntgabe** vor. Dieser Anspruch kommt – wie auch die anderen, sich aus Art. 25 DSG

ergebenden Rechte (3. Kap. B.III., IV.) – nur unter der Voraussetzung zum Zuge, dass eine – aus welchen Gründen auch immer – **widerrechtliche Datenbearbeitung** vorliegt.
Anspruchsberechtigt ist jede Person, die ein **schutzwürdiges Interesse** hat (Art. 25 Abs. 1 DSG). Da es in Art. 25 DSG um Ansprüche in Bezug auf widerrechtlich bearbeitete Daten geht, ergibt sich das schutzwürdige Interesse in aller Regel schon daraus, dass eine widerrechtliche Bearbeitung von Daten in Bezug auf die den Anspruch geltend machende Person zu bejahen ist, deren Folgen durch die Geltendmachung des Art. 25 DSG beseitigt oder zumindest gemildert werden sollen. Denn im Falle einer Bearbeitung von Personendaten, liegt in jedem Fall ein Eingriff in das Grundrecht auf „informationelle Selbstbestimmung" vor (BGE 120 Ia 147 E. 2a, 1. Kap. C.). 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 lit. c BGG – für das Vorliegen eines schutzwürdigen Interesses vorausgesetzte aktuelle rechtliche oder tatsächliche Interesse zu bejahen sein (immer sofern die Person den Anspruch geltend macht, deren Daten widerrechtlich bearbeitet worden sind).
Adressat des Art. 25 DSG ist das **verantwortliche Bundesorgan**.
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 soweit die Voraussetzung der **Widerrechtlichkeit der Datenbearbeitung** vorliegt – jedenfalls stattzugeben ist. Eine Bekanntgabe kann auch deshalb widerrechtlich sein, weil sie in Missachtung einer nach Art. 20 DSG angeordneten Sperre erfolgte.

Das **Verfahren der Ausübung der in Art. 25 DSG garantierten Kontrollrechte** richtet sich nach dem **Verwaltungsverfahrensgesetz** (Art. 25 Abs. 4 DSG). Die Verfügungen des Bundesorgans können beim Bundesverwaltungsgericht angefochten werden; vorher müssen allerdings durch andere Bundesgesetze vorgeschriebene Einsprach- und Beschwerdemöglichkeiten auf Verwaltungsebene ausgeschöpft worden sein.

III. „Bekanntmachungsansprüche"

Art. 25 DSG sieht – neben dem Recht auf Sperrung der Bekanntgabe von Daten – noch diverse **„Bekanntmachungsansprüche"** vor, die unter den bereits erörterten Voraussetzungen (3. Kap. B.II.2.) geltend gemacht werden können:

- Die **Widerrechtlichkeit** der (erfolgten) Bearbeitung ist **festzustellen** (Art. 25 Abs. 1 lit. c DSG). Einem solchen Anspruch ist aber – im Gefolge des bereits erwähnten Erfordernisses eines schutzwürdigen Interesses (3. Kap. B.II.2.) – nur dann stattzugeben, wenn ein entsprechendes Feststellungsinteresse besteht (etwa, wenn es um eine Bearbeitungsmethode geht, die in Zukunft wieder genutzt werden könnte).

- In dem Fall, in dem die (Un-) Richtigkeit von Personendaten nicht klar ist bzw. nicht bewiesen werden kann, hat das Bundesorgan bei den Daten einen entsprechenden **Vermerk** anzubringen (Art. 20 Abs. 2 DSG).

  In Anknüpfung an den Wortlaut der Bestimmung ist davon auszugehen, dass es sich hier nicht nur um ein Recht handelt, das geltend gemacht werden muss, sondern dass dem Bundesorgan (auch) eine entsprechende objektivrechtliche Pflicht obliegt.

- Auf Antrag des Gesuchstellers hat das **Bundesorgan seinen 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 lit. b DSG).

IV. Sonstige Ansprüche im Zuge einer widerrechtlichen Bearbeitung

Schliesslich ist noch auf die sonstigen Ansprüche hinzuweisen, die im Gefolge einer widerrechtlichen Datenbearbeitung geltend gemacht werden können (wobei auch hier ein schutzwürdiges Interesse des Gesuchstellers vorliegen muss, dem Anspruch aber ansonsten, so die Voraussetzung der Widerrechtlichkeit der Datenbearbeitung vorliegt, stattzugeben ist, 3. Kap. B.II.2.):

- Das **widerrechtliche Bearbeiten** von Personendaten ist zu **unterlassen** (Art. 25 Abs. 1 lit. a DSG). Art. 25 Abs. 3 lit. a DSG stellt diesbezüglich noch klar, dass es hier insbesondere um die Berichtigung oder Vernichtung der Daten gehen kann.

  Auch hier handelt es sich nicht nur um ein Recht, das (erst) geltend gemacht werden muss, sondern (auch) um eine objektivrechtliche Pflicht des betroffenen Bundesorgans.

- Die **Folgen eines widerrechtlichen Bearbeitens** sind zu **beseitigen** (Art. 25 Abs. 1 lit. b DSG). Die betroffene Person kann insbesondere das bereits erwähnte (3. Kap. B.III.) Recht auf Mitteilung oder Veröffentlichung des entsprechenden Entscheids geltend machen.

  Es können aber selbstredend immer nur dann (negative) Folgen beseitigt werden, wenn sich die widerrechtliche Bearbeitung von Personendaten tatsächlich zum Nachteil für den Gesuchsteller ausgewirkt hat und wenn diese Folgen durch eine (geeignete) Massnahme beseitigt oder vermindert werden können.
  In Betracht kommen auch etwa Schadensersatz- oder Genugtuungsansprüche, die jedoch auf der Grundlage des Verantwortlichkeitsgesetzes (SR 170.32) geltend zu machen sind.

Lösung Fall 18 (vgl. VPB 68.69):
Die Publikation der hier in Frage stehenden sog. Fahrzeughalterdaten – die als Personendaten im Sinne des Art. 3 lit. a DSG anzusehen sind – ist nach dem Sachverhalt insofern rechtmässig, als die gesetzliche Grundlage ihre Veröffentlichung erlaubt (Art. 19 Abs. 1 DSG). Zumindest die Daten von Fahrzeughalter A sind aber zu sperren, wenn die Voraussetzungen des Art. 20 DSG (Art. 25 DSG kommt mangels Widerrechtlichkeit der Datenbearbeitung nicht zur Anwendung) vorliegen. A ist als betroffene Person anzusehen, da es um die Veröffentlichung seiner Fahrzeughalterdaten geht und diese Daten offenbar systematisch veröffentlicht werden. Fraglich könnte hingegen sein, ob A auch ein schutzwürdiges Interesse daran glaubhaft machen kann, dass seine Daten nicht veröffentlicht werden. Angesichts des Umstandes, dass Art. 20 DSG ausdrücklich ein solches schutzwürdiges Interesse verlangt, liegt dieses nicht schon allein deshalb vor, weil es um die Daten von A geht und er – aus welchen Gründen auch immer – ihre Bekanntmachung unterbinden will. Vielmehr muss der Betroffene ein darüber hinausgehendes schutzwürdiges Interesse an der Nichtbekanntgabe glaubhaft machen. An dieses Erfordernis sind aber im Hinblick auf den Schutzzweck des Art. 20 DSG keine zu hohen Anforderungen zu stellen. Im vorliegenden Fall ist es nicht auszuschliessen, dass die Bekanntgabe der Fahrzeughalterdaten dazu führt, dass bestimmte Fahrzeughalter der Neugier Dritter „ausgeliefert" sind, ganz abgesehen davon, dass die allgemeine Veröffentlichung solcher Daten es grundsätzlich ermöglicht, den betroffenen Fahrzeughalter zu „verfolgen". Eine solche nach allgemeiner Lebenserfahrung bestehende oder zumindest mögliche Beeinträchtigung – wobei ein weitergehender „Beweis", dass sich die erwähnten Befürchtungen tatsächlich realisieren, nicht verlangt werden kann – reicht für ein schutzwürdiges Interesse im Sinne des Art. 20 DSG aus. Es ist insbesondere nicht notwendig, dass ein Grundrechtseingriff oder eine Rechtsverletzung zu befürchten ist; vielmehr ist das blosse, eben nach Art. 20 DSG schutzwürdige Interesse eines Fahrzeughalters daran, dass sich solche, nach der allgemeinen Lebenserfahrung durchaus plausible Beeinträchtigungen nicht realisieren, ausreichend. Da nicht ersichtlich ist, dass die Ausnahmen des Art. 20 Abs. 2, 3 DSG greifen ist dem Antrag auf Sperrung daher stattzugeben.

Fall 19 (vgl. VPB 67.73):
Eine Bundesbehörde, welche Personendaten bearbeitet, ist grundsätzlich dafür verantwortlich, die Richtigkeit der bearbeiteten Daten zu beweisen, wenn diese bestritten wird. Der betroffenen Person obliegt hingegen der Beweis der Unrichtigkeit. Vorliegend ist die Richtigkeit des Geburtsjahres nicht bewiesen. Der ursprüngliche Eintrag stützte sich vielmehr ausschliesslich auf die Angaben des Beschwerdeführers selbst. Nachdem er nunmehr ausdrücklich 1974 als sein richtiges Geburtsjahr bezeichnet und dies immerhin mit einem Dokument belegt, erscheinen erheblich Zweifel an der ursprünglichen Version angebracht. Um das Prinzip der Richtigkeit der bearbeiteten Personendaten gemäss Art. 5 und 25 DSG zu gewährleisten, ist das registrierte Geburtsjahr 1976 des Beschwerdeführers zu löschen. Da im vorliegenden Fall weder die Richtigkeit noch die Unrichtigkeit des vom Beschwerdeführer neu angegebenen Geburtsjahres 1974 mit hinlänglicher Sicherheit bewiesen ist, liegt ein Anwendungsfall von Art. 25 Abs. 2 DSG vor. Bei Bestehen von Zweifel an der Richtigkeit kann die Berichtigung nur dann angeordnet werden, wenn gleichzeitig ein Bestreitungsvermerk angebracht wird. Die Änderung des Geburtsjahres ist – da das „neue“ Geburtsdatum insgesamt wohl plausibler ist – also vorzunehmen, unter Anbringung des Vermerks, dass die Richtigkeit des Datums nicht bewiesen ist.

4. Kapitel Institutionelle Aspekte

Literatur: Maurer-Lambrou/Vogt-HUBER, Art. 26, 27, 28, 30, 31, 32 DSG; EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz; EDÖB-Newsletter „datum"; Tätigkeitsberichte des EDÖB; Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, SR 88.032; 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 der Menschen bei der automatischen Verarbeitung von Personendaten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung vom 19. Februar 2003, SR 03.016; Kommentar zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11).

Eine effektive Anwendung der bislang erörterten datenschutzrechtlichen Vorgaben impliziert auch eine Reihe „institutioneller Vorkehrungen", die auf die eine oder andere Weise sicherstellen sollen, dass die Datenschutzbestimmungen auch tatsächlich eingehalten werden. Diese Kategorie von Normen ergänzt die Rechte der Einzelnen und ist als komplementär zu diesen anzusehen. Im Einzelnen können hier im Wesentlichen drei Aspekte bzw. Mechanismen oder Organe unterschieden werden: der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (A.), die Datenschutzberater (B.) sowie die Pflicht zur Anmeldung von Datensammlungen und das Datensammlungsregister (C.).

A Datenschutz- und Öffentlichkeitsbeauftragter

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (vgl. Art. 26-32 DSG, Art. 30-34 VDSG) soll **Privatpersonen und Bundesorgane im Hinblick auf die Einhaltung der gesetzlichen Datenschutzbestimmungen beaufsichtigen** und **beraten.** Der EDÖB hat weiter die Aufgabe, über die Aspekte des Datenschutzes zu informieren und die Betroffenen zu sensibilisieren.

Die **Stellung des EDÖB** wurde mit der **Revision des DSG** (1. Kap. D.) modifiziert und **gestärkt**. Insbesondere wurde in Art. 27 Abs. 6 DSG neu ein Beschwerderecht gegen Verfügungen von Bundesbehörden, die die Befolgung seiner Empfehlungen ablehnen, eingeführt. Auch verfügt der EDÖB nunmehr über ein eigenes Budget (Art. 26 Abs. 3 DSG).
Die Stellung des EDÖB ergibt sich ansonsten aus Art. 26 Abs. 1, 2 DSG: Er wird vom Bundesrat gewählt (wobei in Zukunft eine Genehmigung durch das Parlament notwendig sein soll, vgl. NZZ v.14.5.2009, 14), erfüllt seine Aufgaben unabhängig (eine Vorgabe, die sich auch aus dem Zusatzprotokoll zur Datenschutzkonvention des Europarates und der Datenschutzrichtlinie, RL 95/46, ergibt, 2. Kap. B.I.3.b), B.II.2.) und ist administrativ (neu) der Bundeskanzlei unterstellt.

Die **wesentlichen Aufgaben des EDÖB** (vgl. Art. 27 ff.) lassen sich durch folgende Punkte zusammenfassen:

- Aufsicht über Bundesorgane;
- Aufsicht über Privatpersonen;
- Beratung von Privatpersonen;
- Unterstützung und Beratung der Organe des Bundes und der Kantone;
- Stellungnahme zu Rechtsvorlagen des Bundes;
- Zusammenarbeit mit in- und ausländischen Datenschutzbehörden;
- Prüfung der Zertifizierungsverfahren nach Art. 11 DSG;
- Information der Öffentlichkeit;

- Führung und Veröffentlichung des Registers der Datensammlung.

Daneben nimmt der EDÖB auch im privatrechtlichen Bereich Aufgaben wahr (Art. 28, 29 DSG), und ihm werden gemäss Art. 32 DSG Aufgaben im Bereich der medizinischen Forschung übertragen.
Seit dem Inkrafttreten des **BGÖ** erfüllt der EDÖB auch im Bereich des Öffentlichkeitsgesetzes verschiedene Aufgaben:

- Information und Beratung von Privaten, die den Zugang zu amtlichen Dokumenten verlangen;
- Beratung der Bundesämter und Departemente bei der Umsetzung des BGÖ;
- Leitung des Schlichtungsverfahrens bei Unstimmigkeiten;
- Abgabe einer schriftlichen Empfehlung zuhanden der Beteiligten;
- Stellungnahme zu Rechtsvorlagen des Bundes, die das Öffentlichkeitsprinzip betreffen.

Im Zusammenhang mit der Tätigkeit der Bundesbehörden kommt der Aufsicht über Bundesorgane (Art. 27 DSG) eine besondere Bedeutung zu: Gemäss **Art. 27 Abs. 1 DSG** übt der EDÖB eine Aufsichtsfunktion gegenüber den **Bundesorganen** (mit Ausnahme des Bundesrates) aus. Dabei handelt es sich um die wichtigste Aufgabe und Kompetenz des EDÖB im öffentlich-rechtlichen Bereich.

Der EDÖB überwacht die Einhaltung des DSG und der übrigen Datenschutzbestimmungen des Bundes durch die Bundesorgane und kann bei Verdacht auf Verletzung des DSG eine Sachverhaltsabklärung, verbunden mit gewissen Informationsbeschaffungsrechten, vornehmen (Art. 27 Abs. 2, 3 DSG) und bei der Feststellung einer solchen, Empfehlungen zur Beseitigung der Widerrechtlichkeit an das betroffene Bundesorgan abgeben (Art. 27 Abs. 4 DSG). Befolgt das betroffene Bundesorgan die Empfehlung nicht, kann der EDÖB die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5 DSG). Beachten das Departement oder die Bundeskanzlei die **Empfehlung** des EDÖB nicht, kann dieser einen entsprechenden Entscheid ans Bundesverwaltungsgericht weiterziehen (Art. 27 Abs. 6 DSG).
Der EDÖB hat neben seiner Aufsichtsfunktion auch eine Informationsfunktion (**Art. 30 DSG**). Er erstattet jährlich einen **Tätigkeitsbericht,** welcher veröffentlicht wird.

B Datenschutzberater

Die **Bundeskanzlei** sowie die einzelnen **Departemente** haben gemäss **Art. 23 VDSG** jeweils einen verwaltungsinternen **Berater für den Datenschutz** zu bezeichnen. Die Aufgabe dieser Berater ist es, die verantwortlichen Organe und Benützer zu **unterstützen,** die Mitarbeiter zu **informieren** und **auszubilden** sowie beim **Vollzug der Datenschutzvorschriften** mitzuwirken (Art. 23 Abs. 1 VDSG). Die Bundesorgane verkehren mit dem EDÖB über den Datenschutzberater (Art. 23 Abs. 3 VDSG).

Diese Pflicht zur Bezeichnung von Datenschutzberatern ist schon deshalb ebenso sinnvoll wie notwendig, als – wie bereits erwähnt (1. Kap. D.) – sich die im Bereich des Datenschutzes in den verschiedenen Tätigkeitsbereichen der Bundesverwaltung zu beachtenden Vorgaben unterscheiden bzw. einer Präzision bedürfen, sind doch jeweils in aller Regel Spezialgesetze einschlägig. Hinzu kommt, dass es bei der Anwendung der (allgemeinen oder spezifischen) Datenschutzbestimmungen häufig auf die genauen Umstände des Einzelfalls und damit auch der betroffenen Materie ankommt, so dass sich auch aus diesem Grund die Bezeichnung von Personen, die sich in jedem Departement speziell mit datenschutzrechtlichen Fragen auseinandersetzen und entsprechende Aufgaben wahrnehmen, aufdrängt.

Zwar kommen den lediglich auf Verordnungsstufe erwähnten Datenschutzberatern keine gesetzlich festgelegten Kontrollaufgaben zu; ebensowenig werden spezifische Anforderungen an die Datenschutzberater formuliert (etwa in Bezug auf Unabhängigkeit). Da der Hintergrund der Einrichtung der Datenschutzberater aber gerade darin besteht, die **Einhaltung der datenschutzrechtlichen Vorgaben in den einzelnen Departementen sicherzustellen** und zu fördern, erscheint es notwendig bzw. zumindest sinnvoll, dass die Datenschutzberater die Gewähr dafür bieten, dass sie die Frage nach der Beachtung der datenschutzrechtlichen Regelungen bei der Tätigkeit des betreffenden Bundesorgans auch tatsächlich unvoreingenommen analysieren und prüfen können. Dies bedingt zweifellos eine gewisse **fachliche Eignung**, aber auch eine geeignete Stellung im Departement, die zumindest eine **gewisse Unabhängigkeit** in Bezug auf die datenschutzrechtlichen Aspekte impliziert.

Daher ist es wohl nicht sinnvoll, wenn die Funktionen des Datenschutzberaters und des Departementinformatikers von ein- und derselben Person wahrgenommen werden. Denn die Interessenkollision zwischen den beiden Funktionen ist offensichtlich, hat doch der Datenschutzberater u.a. darum besorgt zu sein, dass bei der EDV-Systemgestaltung die gesetzlichen Rahmenbedingungen in angemessener Weise berücksichtigt werden. Ähnliches gilt für die Konstellation, bei der diejenigen Stellen, die zentrale Aufgaben im Bereich der Bearbeitung von Personendaten wahrnehmen, gleichzeitig Datenschutzberater sind (vgl. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten, TB 5 74). Allerdings ist darauf hinzuweisen, dass sich aus den gesetzlichen Vorgaben selbst kaum Argumente ergeben, wonach solche Bezeichnungen unzulässig wären.

Will ein Bundesorgan die **Möglichkeit der Nichtanmeldung einer Datensammlung** nach Art. 11a Abs. 5 lit. e DSG nutzen (4. Kap. C.), so sind die Vorgaben des **Art. 12a, 12b VDSG** anwendbar. Danach ist ein sog. **Datenschutzverantwortlicher** zu bezeichnen (worüber der EDÖB zu informieren ist), der durchaus identisch mit dem Datenschutzberater der Verwaltung sein kann. Allerdings formulieren Art. 12a Abs. 2, 12b VDSG **spezifische Anforderungen an den Datenschutzverantwortlichen bzw. den Datenschutzberater**:

- Der Datenschutzverantwortliche darf keine **anderen Tätigkeiten** ausüben, die mit seinen **Aufgaben als Datenschutzverantwortlicher unvereinbar** sind (Art. 12a Abs. 2 VDSG). Auch übt der Datenverantwortliche seine Funktion **fachlich unabhängig** aus und darf keine Weisungen des Inhabers der Datensammlung unterliegen (Art. 12b Abs. 2 lit. a VDSG). In dieser Konstellation müsste also der Datenschutzberater tatsächlich alle Gewähr für Unabhängigkeit bieten, was etwa

nicht gegeben wäre, wenn der Datenschutzberater gleichzeitig der Verantwortliche für die Datensammlung ist.

- Der Datenschutzverantwortliche muss über die **notwendigen Fachkenntnisse** verfügen (Art. 12a Abs. 2 VDSG).
- Die **erforderlichen Ressourcen** müssen zur Verfügung stehen (Art. 12b Abs. 2 lit. b VDSG).
- Der Datenschutzverantwortliche hat Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu **allen Informationen, die er zur Erfüllung seiner Aufgabe benötigt** (Art. 12b Abs. 2 lit. c VDSG).
- Die **Aufgaben des Datenschutzverantwortlichen bzw. Datenschutzberaters** erstrecken sich auf die Prüfung der Vereinbarkeit der Bearbeitung von Personendaten mit den datenschutzrechtlichen Vorgaben, die Formulierung von Empfehlungen im Falle der (möglichen) Verletzung solcher Vorgaben und das Führen einer Liste der Datensammlungen (Art. 12b Abs. 1 VDSG).

C Datensammlungsregister

Art. 11a DSG sieht vor, dass der **EDÖB** ein sog. **Register der Datensammlungen** führt; dieses Register ist allgemein über das Internet einsehbar (Art. 11a Abs. 1 DSG). Das Datensammlungsregister trägt zur **Transparenz** der Datenbearbeitung bei, **erleichtert die Ausübung des Auskunftsrechts** und soll es den betroffenen Personen ermöglichen, die ihnen gesetzlich zustehenden Rechte geltend zu machen. Zudem soll das Register den Datenschutzaufsichtsstellen, insbesondere dem EDÖB, einen **Überblick über die Datenbearbeitungen in der Bundesverwaltung** und in der Privatwirtschaft vermitteln. In diesem Sinn sieht Art. 11a Abs. 2 DSG denn auch vor, dass **Bundesorgane die Pflicht** haben, **Datensammlungen beim EDÖB anzumelden**, wobei diese Anmeldung **vor der Eröffnung** der Datensammlung – also vor der Bearbeitung der ersten Personendaten – zu erfolgen hat (Art. 11a Abs. 4 DSG).

Unter einer **Datensammlung** ist gemäss **Art. 3 lit. g DSG** jeder Bestand von Personendaten zu verstehen, der so aufgebaut ist, dass die **Daten nach betroffenen Personen erschliessbar** sind.
Die bei der **Anmeldung anzugebenden Angaben** sind in Art. 16 Abs. 1 VDSG aufgeführt; sie werden dann auch in das Register der Datensammlungen aufgenommen (Art. 28 Abs. 1 VDSG). Es handelt sich um folgende Angaben (die laufend zu aktualisieren sind, Art. 16 Abs. 2 VDSG):

- Name und Adresse des verantwortlichen Bundesorgans;
- Name und vollständige Bezeichnung der Datensammlung;
- das Organ, bei dem das Auskunftsrecht geltend gemacht werden kann;
- die Rechtsgrundlage und der Zweck der Sammlung;
- Kategorie der bearbeiteten Personendaten;
- Kategorie der Empfänger der Daten;
- Kategorie der an der Datensammlung Beteiligten, das heisst Dritte, die Daten in eine Datensammlung eingeben und verändern dürfen.

Die **Anmeldepflicht** kennt aber auch **Ausnahmen**, die einerseits in **Art. 11a Abs. 5 DSG**, andererseits in **Art. 18 VDSG** – der eine im Gesetz enthaltene Ermächtigung aufgreift – vorgesehen sind. Gemäss Art. 11a Abs. 5 DSG muss eine Datensammlung u.a. (auf die nur für Private zur Anwendung kommenden Ausnahmen wird nicht hingewiesen) **nicht angemeldet** werden, wenn

- der Bundesrat die Bearbeitung von der Anmeldepflicht ausgenommen hat, weil sie die Rechte der betroffenen Person nicht gefährdet (vgl. Art. 18 VDSG);
- der Inhaber der Datensammlung die Daten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet und keine Daten an Dritte weitergibt, ohne dass die betroffene Person davon Kenntnis hat;
- der Inhaber einer Datensammlung einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (4. Kap. B.);
- der Inhaber der Datensammlung aufgrund eines Zertifizierungsverfahrens nach Art. 11 DSG ein Datenschutz-Qualitätszeichen erworben hat und das Ergebnis der Bewertung dem EDÖB mitgeteilt wurde.

  Bei der **Zertifizierung** handelt es sich um eine standardisierte Überprüfung (durch eine anerkannte und unabhängige Zertifizierungsstelle) von System, Organisation und Verfahren einer Einheit (u.a. eines Bundesorgans) in Bezug auf die Frage der Einhaltung gewisser Qualitätsstandards (zu denen

jedenfalls die gesetzlichen Mindestvorgaben gehören müssen). Das Datenschutzniveau wird dann mit einem „Datenschutz-Qualitätszeichen“ bescheinigt (Art. 11 Abs. 2 DSG). Die Einzelheiten sind in der Verordnung über die Datenschutzzertifizierungen (VDSZ, SR 235.13) geregelt.

Art. 18 Abs. 1, 2 VDSG nennt weitere **Ausnahmen von der Anmeldepflicht** von Datensammlungen (sofern diese ausschliesslich für **verwaltungsinterne Zwecke** verwenden werden) der Bundesorgane:

- Korrespondenzregistraturen;
- Datensammlungen von Lieferanten oder Kunden, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten;
- Adresssammlungen, die einzig der Adressierung dienen, soweit sie keine besonders schützenswerten oder Persönlichkeitsprofile enthalten;
- Listen für Entschädigungszahlungen und Buchhaltungsunterlagen;
- Hilfsdatensammlungen für die Personenverwaltung des Bundes, wenn sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten;
- Bibliotheksdatensammlungen;
- Datensammlungen, die beim Bundesarchiv archiviert sind;
- Datensammlungen, die der Öffentlichkeit in Form von Verzeichnissen zugänglich gemacht werden;
- Datensammlungen, deren Daten ausschliesslich zu nicht personenbezogenen Zwecken verwendet werden, namentlich in der Forschung, der Planung und der Statistik.

Art. 18 Abs. 3 VDSG hält ausdrücklich fest, dass das zuständige Bundesorgan verpflichtet ist, alle Massnahmen zu treffen, die erforderlich sind, um die Angaben gemäss Art. 16 Abs. 1 VDSG auch dann dem EDÖB und den betroffenen Personen auf Gesuch hin mitteilen zu können, wenn eine Datensammlung nicht der Anmeldepflicht unterliegt.

5. Kapitel Schlussbetrachtung: zu den Herausforderungen des Datenschutzrechts

Datenschutz ist – wie diese Einführung wohl illustrieren konnte – eine **komplexe Materie**, nicht nur, weil die einschlägigen rechtlichen Grundlagen mitunter unübersichtlich sind, sondern auch und vor allem, weil es sich um ein Gebiet handelt, in dem **verschiedene Interessen** aufeinander stossen und miteinander abgewogen werden müssen, dies unter **Beachtung der einschlägigen (verfassungs-) rechtlichen Vorgaben**. Weiter lassen die **technischen Entwicklungen** die Frage des Datenschutzes in einem neuen Licht erscheinen, stehen doch heute diverse technische Möglichkeiten des „Eindringens" in die Privatsphäre zur Verfügung, deren Potentiale zur Verfolgung verschiedener öffentlicher Ziele noch nicht ausgeschöpft erscheinen, womit aber auch eine entsprechende Beeinträchtigung der Privatsphäre verbunden ist, ganz abgesehen davon, dass immer mit „Datenpannen" gerechnet werden muss. Schliesslich ist daran zu erinnern, dass immer wieder besonderes wichtige öffentliche Interessen geltend gemacht werden, die **scheinbar in jedem Fall über datenschutzrechtliche Anliegen stehen** (sollen); Stichwörter in diesem Zusammenhang sind die innere Sicherheit im Allgemeinen und die Kriminalitätsbekämpfung im Besonderen.
Angesichts dieser Feststellungen ist es immer wieder hilfreich, sich auf einige Grundprinzipien nicht nur des Datenschutzes, sondern auch des demokratischen Rechtsstaats zu besinnen, wobei in unserem Zusammenhang in erster Linie folgende Aspekte von Bedeutung sein dürften:

- Datenschutz weist – wie bereits eingangs (1. Kap. A.) erwähnt – eine **grundrechtliche Dimension** auf, ist aber auch im eminent **öffentlichen Interesse**, so dass er keinesfalls zur beliebigen Disposition steht, sondern entsprechende Beeinträchtigungen strengen rechtlichen Regeln zu genügen haben.

- Unabhängig davon, ob eine Person „etwas zu verbergen hat", hat sie ein **Grundrecht auf Schutz ihrer informationellen Selbstbestimmung**; jeder staatliche Eingriff in diese ist **rechtfertigungsbedürftig** (wobei die Anforderungen selbstredend differieren).

- In diesem Sinn sind **„unnötige" Datensammlungen und Datenbearbeitungen** zu vermeiden; es sind also so wenig wie möglich Bearbeitungsvorgänge zu tätigen, was sich schon aus dem Verhältnismässigkeitsgrundsatz ergibt.

- Bei der Anwendung des **Verhältnismässigkeitsgrundsatzes** – der im Datenschutz eine überragende Rolle spielt – ist den verfassungsrechtlichen Wertungen hinreichend Rechnung zu tragen. Dies gilt auch bei wichtigen öffentlichen Interessen, wie der Gewährleistung der inneren Sicherheit. Der Staat muss sich in seinem Agieren an den rechtsstaatlichen Grundsätzen messen lassen.

- **Gesetzliche Grundlagen** sind möglichst genau zu formulieren.

Die zentrale Herausforderung des Datenschutzrechts und insbesondere seiner Anwendung ist vor diesem Hintergrund darin zu sehen, die in diesem Band erörterten **Grundsätze des datenschutzrechtlichen Standards** in der **Rechtsordnung umfassend zur Geltung zu bringen**, was einerseits im Rahmen der Rechtsetzung (durch Parlament und Regierung als Verordnungsgeber), andererseits aber auch im Rahmen der Rechtsanwendung durch

Behörden und Gerichte zu geschehen hat, so dass die erwähnte grundsätzliche Bedeutung des Datenschutzes auch bei jeder einzelnen Datenbearbeitung präsent ist, insbesondere, wenn diese Bearbeitung durch staatliche Behörden erfolgt. Diese „Operationalisierung" des Datenschutzes in der gesamten Rechtsordnung impliziert auch und gerade, dass für die diversen neueren Probleme in diesem Zusammenhang **sachgerechte und den verfassungsrechtlichen Anforderungen entsprechende Konkretisierungen** – sowohl auf der Rechtsetzungs- als auch auf der Rechtsanwendungsebene – gefunden werden.

So sind etwa auch im Rahmen der Wahrung der inneren Sicherheit die Voraussetzungen eines Eingriffs in die Privatsphäre jedenfalls sehr genau zu umschreiben und bei Eingriffen präventiver Natur ist u.E. grösste Zurückhaltung zu üben. Weiter sind auch hier Auskunfts- und Berichtigungsrechte – wenn auch ggf. eingeschränkt – zu gewähren. Im Falle der „Internationalisierung" des Datenaustauschs (etwa im Rahmen polizeilicher Zusammenarbeit) ist jeweils darauf zu achten, dass die Internationalisierung des Datenaustauschs auch mit einer angemessenen Internationalisierung des Datenschutzstandards einhergeht, wobei Zweckbindung und Verhältnismässigkeit eine besondere Rolle spielen dürfen.
Ein weiteres Beispiel ist die Konkretisierung datenschutzrechtlicher Standards in Bezug auf (neuere) technische Entwicklungen: Die Präzisierung der im Einzelnen aus technischer Sicht einzuhaltenden Anforderungen, die sich ihrerseits aus den allgemeinen datenschutzrechtlichen Grundsätzen ableiten lassen, dürfte hier von grosser Bedeutung sein.

Literatur

AUER, ANDREAS/MALINVERNI, GIORGIO/HOTTELIER, MICHEL: Droit constitutionnel suisse, vol. II. Les droits fondamentaux, 2ème éd., Berne 2006.

BAERISWYL, BRUNO: Entwicklungen im Datenschutzrecht / Le point sur le droit de la protection des données, SJZ 2008, 459 ff.

BRITZ, GABRIELE: Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1 ff.

COTTIER, BERTIL: La révision de la loi fédérale sur la protection des données : mieux vaut tard que jamais, Jusletter, 17. Dezember 2007.

DAMMANN, ULRICH/SIMITIS, SPIROS: EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997.

DRECHSLER, CHRISTIAN: Die Revision des Datenschutzrechts, AJP 2007, 1471 ff.

EHMANN, EUGEN/HELFRICH, MARKUS: EG-Datenschutzrichtlinie, Kurzkommentar, Köln 1999.

EHRENZELLER, BERNHARD/MASTRONARDI, PHILIPPE/SCHWEIZER, RAINER J./VALLENDER, KLAUS A. (Hrsg.): Die schweizerische Bundesverfassung, Kommentar, 2. Aufl., 2 Bände, Zürich u.a. 2008 (zit. Ehrenzeller/Mastronardi/Schweizer/Vallender-BEARBEITER).

EPINEY, ASTRID: Datenschutz und „Bilaterale II", SJZ 2006, 121 ff.

EPINEY, ASTRID/FREIERMUTH, MARIANNE (Hrsg.): Datenschutz in der Schweiz und in Europa – La protection des données en Suisse et en Europe, Fribourg 1999.

EPINEY, ASTRID/HOBI, PATRICK (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, Zürich 2009.

EPINEY, ASTRID/HOFSTÖTTER, BERNHARD/MEIER, ANNEKATHRIN/THEUERKAUF, SARAH: Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen. Zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, Zürich 2007.

EPINEY, ASTRID/MEIER, ANNEKATHRIN/EGBUNA-JOSS, ANDREA: Schengen/Dublin, in: Thürer, Daniel/Weber, Rolf H./Portmann, Wolfgang/Kellerhals, Andreas (Hrsg.), Bilaterale Verträge I & II Schweiz – EU. Handbuch, Zürich 2007, 903 ff.

EPINEY, ASTRID/THEUERKAUF, SARAH (Hrsg.), Datenschutz in Europa und die Schweiz / La protection des données en Europe et la Suisse, Zürich 2006.

FLÜCKIGER, ALEXANDRE/AUER, ANDREAS: La vidéosurveillance sous l'oeil de la constitution, AJP 2006, 924 ff.

FRENZ, WALTER: Europäischer Datenschutz und Terrorabwehr, EuZW 2009, 6 ff.

FÜZESSÉRY MINELLI, SIMONE/BRUNNER, STEPHAN: La protection des données et les Accords Schengen/Dublin, in: Kaddous, Christine/Jametti Greiner, Monique (Hrsg.), Accords bilatéreux II Suisse – UE et autres accords récents / Bilaterale Abkommen II Schweiz-EU und andere neue Abkommen, Genf u.a. 2006, 425 ff.

GRABENWARTER, CHRISTOPH: Europäische Menschenrechtskonvention, 3. Aufl., München u.a. 2008.

HÄFELIN, ULRICH/HALLER, WALTER/KELLER, HELEN: Schweizerisches Bundesstaatsrecht, 7. Aufl., Zürich u.a. 2008.

HUBER, RENÉ: Die Teilrevision des Eidgenössischen Datenschutzgesetzes - ungenügende Pinselrenovation, recht 2006, 205 ff.

KIENER, REGINA/KÄLIN, WALTER: Grundrechte, Bern 2007.

MAURER-LAMBROU, URS/VOGT, NEDIM PETER (Hrsg.): Basler Kommentar, Datenschutzgesetz, 2. Aufl., Basel u.a. 2006 (zitiert: Maurer-Lambrou/Vogt-BEARBEITER).

MÜLLER, JÖRG PAUL/SCHEFER, MARKUS: Grundrechte in der Schweiz im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008.

PAGE, GÉRALD: Le droit d'accès dans la Jurisprudence de la Commission fédérale de la protection des données, ZBl. 2007, 380 ff.

ROSENTHAL, DAVID/JÖHRI, YVONNE: Handkommentar zum Datenschutzgesetz, Zürich 2008 (zitiert: BEARBEITER, Handkommentar).

ROßNAGEL, ALEXANDER (Hrsg.): Handbuch Datenschutzrecht, München 2003 (zitiert: Roßnagel-BEARBEITER).

ROST, MARTIN: Die EU-DLR aus Sicht des Datenschutzes, RDV 2008, 231 ff.

RUDIN, BEAT: Datenschutzgesetze – fit für Europa, Zürich u.a. 2007.

RUDIN, BEAT: Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ 2009, 1 ff.

SCHEFER, MARKUS: Öffentlichkeit und Geheimhaltung in der Verwaltung, in: Epiney, Astrid/Hobi, Patrick (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, Zürich 2009, 67 ff.

SCHWAB, KARIN: Grenzüberschreitende Bekanntgabe von Personendaten, SJZ 2004, 125 ff.

SCHWEGLER, IVO: Datenschutz im Polizeiwesen von Bund und Kantonen, Bern 2001.

SCHWEITER, RAINER: Die Revision des Datenschutzgesetzes: Hintergrund und Überblick, in: Epiney, Astrid/Hobi, Patrick (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, Zürich 2009, 29 ff.

THEUMANN, GÉRALDINE: Etat de la jurisprudence en matière d'accès aux données personnelles pour les requérantes d'asile au niveau cantonal et au niveau fédéral (2005-2008), Asyl 4/2008, 4 ff.

WALTER, JEAN-PHILIPPE: La loi fédérale du 19 juin 1992 sur la protection des données, AJP/PJA 1993, 52 ff.

WALTER, JEAN-PHILIPPE: Communication de données personnelles à l'étranger, in: Astrid Epiney/Patrick Hobi (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, Zürich 2009, 99 ff.

WEBER, ROLF H./THÜRER, DANIEL/ZÄCH, ROGER (Hrsg.): Datenschutz im europäischen Umfeld, Zürich 1995.

WERMELINGER, AMÉDÉO/SCHWERI, DANIEL: Teilrevision des Eidgenössischen Datenschutzrecht s- Es nützt nicht viel, schadet es etwas?, Jusletter, 3. März 2008.

ZERDICK, THOMAS: Europäisches Datenschutzrecht – neuere Rechtsprechung des EuGH, RDV 2009, 56 ff.

ZILKENS, MARTIN: Europäisches Datenschutzrecht – Ein Überblick, RDV 2007, 196 ff.

Materialien

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413.

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 vom 19. Februar 2003, BBl 2003 2101.

Kommentar zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11), www.edoeb.admin.ch /org/00828/index.html?download=M3wBPgDB/bKbXrZ6lhuDZz8mMps2gpKfo&lang=de, zuletzt konsultiert am 8.6.2009.

EDÖB, Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung, http://www.edoeb.admin.ch/dokumentation/00445/00472/00934/index.html?lang=de, zuletzt konsultiert am 8.6.2009.

EDÖB, Leitfaden über die Rechte der betroffenen Person bei der Bearbeitung von Daten, http://www.edoeb.admin.ch/dokumentation/00445/00472/00576/index.html?lang=de, zuletzt konsultiert am 8.6.2009.

EDÖB, Merkblatt: Die Datenübermittlung ins Ausland kurz erklärt, http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de, zuletzt konsultiert am 28.5.2009.

EDÖB-Newsletter „datum“, http://www.edoeb.admin.ch/ dokumentation/00445/00471/01402/index.html?lang=de, zuletzt konsultiert am 8. 6. 2009

EDÖB, Erläuterung zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, Dokument des EDÖB, http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de, zuletzt konsultiert am 28.5.2009.

EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des DSG, 10. Oktober 2007, http://www.edoeb.admin.ch/themen/00794/00819/01086/index.html?lang=de, zuletzt konsultiert am 26.5.2009.

EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, 1994.

EDÖB, Tätigkeitsberichte, http://www.edoeb.admin.ch/dokumentation/00445/00509/01255/index.html?lang=de,zuletzt konsultiert am 15.6.2009.

Rechtsprechungsverzeichnis

A EGMR

EGMR, Urt. v. 6.9.1978, EuGRZ 1979 (Klass u.a./Deutschland).
EGMR, Urt. v. 26.3.1987, Serie A, Bd. 116 (Leander/Schweden).
EGMR, Urt. v. 26.2.1997, RJD 1997-I (Z/Finnland).
EGMR, Urt. v. 16.2.2000, RJD 2000-II (Amann/Schweiz).
EGMR, Urt. v. 4.5.2000, RJD 2000-V (Rotaru/Rumänien).

B EuGH

EuGH, verb. Rs. C-465/00, C-138/01, C-139/01 (Österreichischer Rundfunk u.a.), Slg. 2003, I-4989.
EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, I-12971.
EuGH, Rs. C-301/06 (Irland/EP und Rat), Urt. v. 10.2.2009
EuGH, Rs. C-275/06 (Promisicae), Slg. 2008, I-271.
EuGH, Rs. C-524/06 (Huber), Urt. v. 16.12.2008.
EuGH, Rs. C-73/07 (Satakunnan Markkinapörssi und Stamedia), Urt. v. 16.12.2008.
EuGH, Rs. C-553/07 (Rijkeboer), Urt. v. 7.5.2009.

C Bundesgericht

BGE 120 Ia 147
BGE 122 II 204
BGE 122 I 360
BGE 123 II 534
BGE 123 II 542
BGE 124 I 176
BGE 124 III 170
BGE 125 II 225
BGE 125 II 321
BGE 125 II 473
BGE 125 II 476
BGE 126 II 126
BGE 127 V 219
BGE 131 II 413
BGE 133 V 359
BGE 2A.424/2000
BGE 2A.534/2001
BGE 1A.6/2001
BGE 1A.295/2005
BGE 1C.44/2008

D Bundesverwaltungsgericht

A-7372/2006, vom Bundesgericht bestätigt in Urteil 1C.201/2007
A-7367/2006
A-7369/2006
A-7368/2006
A-4202/2007
A-2482/2007
A-420/2007
A-5737/2007
A-1711/2007
A-3764/2008
D-2831/2008
A-3144/2008
A-6067/2008
A-7307/2008
A-6559/2008
A-7183/2008
A-5287/2008
A-50/2009

Verzeichnis nützlicher Links

www.edoeb.admin.ch
www.edps.europa.eu
www.datenschutz.zug.ch
www.datenschutz.ch
www.privatim.ch
www.digma.info
www.fir.unisg.ch/datenschutz
www.unifr.ch/euroinstitut

Abkürzungen

ABl.	Amtsblatt der Europäischen Union (bis 1.2.2002: Amtsblatt der Europäischen Gemeinschaften)
Abs.	Absatz
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung, SR 831.10
AJP	Aktuelle Juristische Praxis
AmtlBull.	Amtliches Bulletin
Art.	Artikel
AsylG	Asylgesetz, SR 142.31
Aufl.	Auflage
AUPER	Automatisiertes Personenregistratursystem
AUPER-V	Verordnung über das automatisierte Personenregistratursystem AUPER, SR 142.315
AVIG	Arbeitslosenversicherungsgesetz, SR 837.0
AVV	Verordnung über die Arbeitsvermittlung und den Personalverleih, SR 823.111
BBl	Bundesblatt (Schweiz)
Bd.	Band
BGE	Bundesgerichtsentscheid
BGG	Bundesgerichtsgesetz, SR 173.110
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung, SR 152.3
BinfV	Verordnung über die Informatik und die Telekommunikation in der Bundesverwaltung, SR 172.010.58
BstatG	Bundesstatistikgesetz, SR 431.01
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft, SR 101
bzw.	beziehungsweise
d.h.	das heisst
Doc.	Document
DSG	Bundesgesetz über den Datenschutz, SR 235.1
EBG	Eisenbahngesetz, SR 742.101
EBV	Eisenbahnverordnung, SR 742.141.1
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
EP	Europäisches Parlament
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EuGRZ	Europäische Grundrechtezeitschrift
EUV	Vertrag zur Gründung der Europäischen Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f./ff.	folgende

FMG	Fernmeldegesetz, SR 784.10
Ggf.	gegebenenfalls
Hrsg.	Herausgeber
i.e.S.	im engeren Sinne
IKT	Informations- und Kommunikationstechniken
IRB	Informatikrat Bund
ISB	Informationsstrategieorgan Bund
IschV	Verordnung über den Schutz von Informationen des Bundes, SR 510.411
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinne
Kap.	Kapitel
lit.	litera
m.a.W.	mit anderen Worten
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
o.ä.	oder ähnliche(s)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OR	Obligationenrecht, SR 220
RDV	Recht der Datenverarbeitung
RJD	Reports of Judgments and Decisions; Entscheidungssammlung des EGMR (seit 1996).
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
RVOG	Regierungs- und Verwaltungsorganisationsgesetz, SR 172.010
RVOV	Regierungs- und Verwaltungsorganisationsverordnung, SR 172.010.1
s.	siehe
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs, SR 281.1
SIS	Schengener Informationssystem
SJZ	Schweizerische Juristen-Zeitung
Slg.	Sammlung der Rechtsprechung des EuGH
sog.	sogenannt
StGB	Schweizerisches Strafgesetzbuch, SR 311.0
SR	Systematische Sammlung des Bundesrechts
TB	Tätigkeitsbericht
u.a.	unter anderem
UA	Unterabsatz
Urt.	Urteil
VDSG	Verordnung zum Bundesgesetz über den Datenschutz, SR 235.11
vgl.	vergleiche
Vo.	Verordnung
VPB	Verwaltungspraxis der Bundesbehörden

VTE	Verordnung über die Zulassung von Triebfahrzeugführenden der Eisenbahnen, SR 742.141.142.1
VwVG	Bundesgesetz über das Verwaltungsverfahren, SR 172.021
WIsB	Weisungen des IRB über die Informationssicherheit in der Bundesverwaltung
z.B.	zum Beispiel
ZBl.	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
ZGB	Schweizerisches Zivilgesetzbuch, SR 210
Ziff.	Ziffer

Die vorliegende Einführung in das Datenschutzgesetz des Bundes vermittelt die wesentlichen Grundsätze und die Systematik des für die Bundesorgane massgeblichen Datenschutzrechts, wobei sie einerseits Aspekte, die zum allgemeinen Verständnis des Datenschutzes unerlässlich sind, erläutert; andererseits werden Bereiche erörtert, die spezifisch für mit der Datenbearbeitung befassten Bundesorgane von Bedeutung sind. Die datenschutzrechtlichen Vorgaben in Bezug auf Datenbearbeitung durch Private bleiben im Wesentlichen ausgespart.

In einem ersten Kapitel werden die Grundlagen des Datenschutzrechts skizziert. Das zweite Kapitel bildet den Schwerpunkt und widmet sich den Vorgaben für die Datenbearbeitung durch Bundesorgane und den Vorgaben der Datenübermittlung ins Ausland. In zwei weiteren Kapiteln geht es um die Rechte der Einzelnen sowie die institutionellen Aspekte, bevor in einem letzten Kapitel einige Gedanken zu den Herausforderungen des Datenschutzrechts formuliert werden.

La présente introduction à la loi fédérale sur la protection des données expose les principes essentiels ainsi que la systématique des dispositions du droit de la protection des données applicables aux organes fédéraux. Elle décrit d'une part les aspects essentiels à une compréhension générale du droit de la protection des données et aborde d'autre part des domaines qui ont une importance spécifique pour le traitement de données par les différents organes fédéraux. Les normes concernant le traitement de données par des personnes privées sont pour l'essentiel laissées de côté.

Le premier chapitre esquisse les bases du droit de la protection des données. Le second chapitre, qui est le principal, traite des prescriptions concernant le traitement de données par des organes fédéraux ainsi que la communication de données à l'étranger. Les deux chapitres suivants sont consacrés aux droits des particuliers et aux aspects institutionnels. Finalement, quelques réflexions concernant les enjeux du droit de la protection des données sont formulées dans le dernier chapitre.

Astrid Epiney, Prof. Dr. iur., LL.M., Lehrstuhl für Europarecht, Völkerrecht und öffentliches Recht der Universität Freiburg i.Ue., geschäftsführende Direktorin des Instituts für Europarecht der Universitäten Bern, Freiburg und Neuenburg.

Tamara Civitella, lic.iur., RA, Assistentin, Institut für Europarecht der Universität Freiburg i.Ue.

Patrizia Zbinden, MLaw, Assistentin, Institut für Europarecht der Universität Freiburg i.Ue.